BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-124960

(43)Date of publication of application : 26.04.2002

(51)Int.Cl. H04L 12/28
H04L 9/08

(21)Application number : 2000-315395

(22)Date of filing : 16.10.2000

(71)Applicant : LINK EVOLUTION CORP

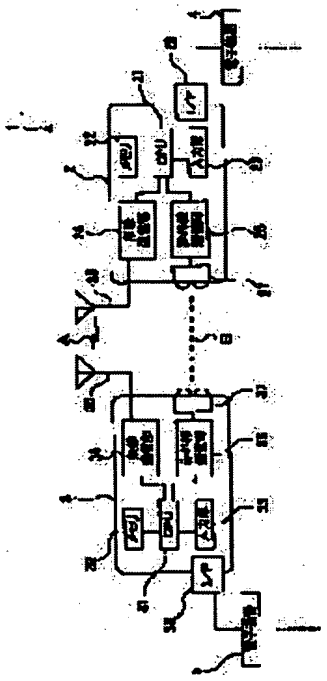
(72)Inventor : KITAKADO KENTARO

(54) COMMUNICATION DEVICE, COMMUNICATION SYSTEM, AND COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To improve reliability in security without losing the convenience of radio communication when transmitting or receiving data between a plurality of electronic equipment by radio communication.

SOLUTION: In a communication system 1, data are transmitted or received via a radio communication link A conforming to the Bluetooth standard and an infrared communication link B between communication devices 2 and 3. The communication device 2 transmits original encryption information retained in a memory 22 to the communication device 3 via the infrared communication link B, and the communication device 3 retains the transmitted original encryption information in a memory 32. Then, when information is to be transmitted via the radio communication link A from the communication device 2 to the communication device 3, information that is encrypted based on the original encryption information in the memory 22 is transmitted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention relates to the communication device corresponding to two or more different communication modes, communication system equipped with this communication device, and the correspondence procedure in this communication system.
[0002]
[Description of the Prior Art] When data communication was conventionally performed among electronic equipment, such as a personal computer, PDA (Personal Digital Assistant), and a portable telephone, the technique of connecting mutual electronic equipment by the cable was used. However, in order that the technique using the cable might require the time and effort which connects a cable to electronic equipment and might carry a cable, it was inconvenient. Then, recently, radio technology came to be used for the data communication between two or more electronic equipment.
[0003] Especially, in recent years, in order to raise the convenience of electronic equipment, it is decided upon two or more radio specification which is rich in compatibility. If the communication device according to these telecommunications standards is used, data communication can be easily performed among various electronic equipment.
[0004]
[Problem(s) to be Solved by the Invention] However, when data communication was performed using radio technology, it needed to be cautious of disclosure of data. Especially when proportionate to the telecommunications standard which can communicate among various devices, it needed to take care that data were not accidentally received by other unrelated devices. Thus, in the data communication using radio technology, it had become a technical problem to improve the reliability on security.
[0005] The technical problem of this invention is raising the reliability on security, without spoiling the convenience of radio, when transmitting and receiving data by radio among two or more electronic equipment.
[0006]
[Means for Solving the Problem] this invention is equipped with the following features in order to solve such a technical problem. In addition, parenthesis writing shows the composition corresponding to the gestalt of operation as an example during explanation of the means shown below. A sign etc. is a drawing reference mark mentioned later.
[0007] The 1st means of communications to which the communication device (2) of invention according to claim 1 transmits and receives a radio signal (for example, Radio Communications Department 24 which shows drawing 1), The 2nd means of communications which transmits and receives a signal by different communication mode from this 1st means of communications (for example, infrared-ray-communication section 26 shown in drawing 1), A key information maintenance means to hold encryption key information (for example, memory 22 which has the primitive encryption information storing field 101 shown in drawing 2), A key information transmission-control means to make the encryption key information held at this key information maintenance means transmit to other

communication devices by the 2nd means of communications of the above (for example, CPU21 which performs processing shown in drawing 3 (a)), It is characterized by enciphering information based on the encryption key information held at the aforementioned key information maintenance means, and having the communications control means (for example, CPU21 which performs processing shown in drawing 5) to which it is made to transmit by the 1st means of communications of the above.

[0008] According to this invention according to claim 1, it has the 1st means of communications which transmits and receives a radio signal, and the 2nd means of communications which transmit and receive a signal by different communication mode from this 1st means of communications. by the key information maintenance means By control of a key information transmission-control means, while transmitting to other communication devices by the 2nd means of communications, the encryption key information which held encryption key information and was held at this key information maintenance means Since information is enciphered by control of a communications control means based on the encryption key information held at the key information maintenance means and it transmits by the 1st means of communications The information transmitted by this communication device is receivable only by the communication device which received the encryption key information transmitted by the 2nd means of communications. Thereby, the reliability on security is securable about the radio by the 1st means of communications. Especially when the radio by the 1st means of communications applies to the radio method with which specification and specification are exhibited, or it spreads widely like for example, the Bluetooth specification, and compatibility is maintained correspondingly, possibility that information will be received by the unrelated communication device cannot be denied. However, if this invention is applied, it can limit only to the communication device which received the encryption key information to which a communicative partner is transmitted by the 2nd means of communications. therefore, physical relationship with the equipment of a communications partner is comparatively free -- etc. -- without spoiling the convenience of radio, informational secrecy nature can be held and the reliability on security can be secured

[0009] Invention according to claim 2 is characterized by to have further a communication refusal means (for example, CPU21 which performs processing shown in Step S45 of drawing 5) refuse transmission and reception of the radio signal by the 1st means of communications of the above, to the external communication device which does not hold the same encryption key information as the encryption key information held at the aforementioned key information maintenance means in a communication device according to claim 1.

[0010] According to invention according to claim 2, the communication device which serves as a communicative partner since transmission and reception of the radio signal according to the 1st means of communications by the communication refusal means to the external communication device which does not hold the same encryption key information as the encryption key information held at the key information maintenance means are refused can be limited strictly, and informational secrecy can be held more certainly.

[0011] Invention according to claim 3 transmits and receives a radio signal in a communication device according to claim 1 or 2 by the communication mode to which the 1st means of communications of the above applied to the Bluetooth (Bluetooth) specification correspondingly, and the 2nd means of communications of the above is characterized by transmitting and receiving a radio signal by the communication mode which used the infrared signal.

[0012] Since the 1st means of communications transmits and receives a radio signal by the communication mode according to the Bluetooth (Bluetooth) specification and the 2nd means of communications transmits [according to invention according to claim 3] and receives a radio signal by the communication mode which used the infrared signal, while specification is exhibited widely and it is rich in convenience, positive information secrecy can secure informational secrecy nature in the radio of the difficult Bluetooth (Bluetooth) specification. Since the communication mode which used the infrared signal for the 2nd means of communications especially is used, the 2nd low-cost[the miniaturization of means of communications, lightweight-izing, and]-izing and power-saving are possible, and it can realize easily. Moreover, in the communication mode using the infrared signal, since a communication

device needs to approach mutually and it is necessary to counter within a predetermined solid angle, informational secrecy nature can be raised further.

[0013] Invention according to claim 4 Transmitting-side equipment (for example, communication device 2 shown in drawing 1), and receiving-side equipment It is the communication system (1) which it comes to have. (For example, communication device 3 shown in drawing 1) The aforementioned transmitting-side equipment The 1st means of communications which transmits and receives a radio signal (for example, Radio Communications Department 24 which shows drawing 1), The 2nd means of communications which transmits and receives a signal by different communication mode from this 1st means of communications (for example, infrared-ray-communication section 26 shown in drawing 1), A key information maintenance means to hold encryption key information (for example, memory 22 which has the primitive encryption information storing field 101 shown in drawing 2), A key information transmission-control means to make the encryption key information held at this key information maintenance means transmit to the aforementioned receiving-side equipment by the 2nd means of communications of the above (for example, CPU21 which performs processing shown in drawing 3 (a)), Information is enciphered based on the encryption key information held at the aforementioned key information maintenance means. It has the communications control means (for example, CPU21 which performs processing shown in drawing 5) made to transmit to the aforementioned receiving-side equipment by the 1st means of communications of the above. the aforementioned receiving-side equipment A key information receiving means to receive the encryption key information transmitted by the 2nd means of communications which the aforementioned transmitting-side equipment has (for example, the infrared-ray-communication section 36 shown in drawing 1 and CPU31 which performs processing shown in drawing 3 (b)), A receiving key information maintenance means to hold the encryption key information received by this key information receiving means (for example, memory 32 shown in drawing 1), It is characterized by having an encryption information receiving means (for example, Radio Communications Department 34 which shows drawing 1) to receive the information transmitted by the 1st means of communications which the aforementioned transmitting-side equipment has.

[0014] According to invention according to claim 4, it is the communication system which comes to have transmitting-side equipment and receiving-side equipment. transmitting-side equipment It has the 1st means of communications which transmits and receives a radio signal, and the 2nd means of communications which transmit and receive a signal by different communication mode from this 1st means of communications. By the key information transmission-control means, while making it transmit to receiving-side equipment by the 2nd means of communications, the encryption key information held encryption key information by the key information maintenance means, and was held at the key information maintenance means By control of a communications control means, information is enciphered based on the encryption key information held at the key information maintenance means, and it transmits to receiving-side equipment by the 1st means of communications. receiving-side equipment A key information receiving means receives the encryption key information transmitted by the 2nd means of communications which transmitting-side equipment has. The encryption key information received by the key information receiving means is held by the receiving key information maintenance means, and an encryption information receiving means receives the information transmitted by the 1st means of communications which transmitting-side equipment has.

[0015] Moreover, the 1st means of communications to which invention according to claim 8 transmits and receives a radio signal (for example, Radio Communications Department 24 which shows drawing 1), The transmitting-side equipment which has the 2nd means of communications (for example, infrared-ray-communication section 26 shown in drawing 1) which transmits and receives a signal by different communication mode from this 1st means of communications (for example, communication device 2 shown in drawing 1), It is a correspondence procedure in the communication system (1) which comes to have receiving-side equipment (for example, communication device 3 shown in drawing 1). with the aforementioned transmitting-side equipment With the process which transmits encryption key information to the aforementioned receiving-side equipment by the 2nd means of communications of the

above, and the aforementioned receiving-side equipment It is characterized by including the process which receives and memorizes the encryption key information transmitted by the 2nd means of communications which the aforementioned transmitting-side equipment has, and the process which enciphers information based on the aforementioned encryption key information with the aforementioned transmitting-side equipment, and is transmitted to the aforementioned receiving-side equipment by the 1st means of communications of the above.

[0016] Therefore, the information transmitted by transmitting-side equipment is receivable with receiving-side equipment. Thereby, the reliability on security is securable about the radio in the communication system using the 1st means of communications which transmitting-side equipment has. Especially when the radio by the 1st means of communications applies to the radio method with which specification and specification are exhibited, or it spreads widely like for example, the Bluetooth specification, and compatibility is maintained correspondingly, possibility of being received by the unrelated communication device cannot be denied. However, if this invention is applied, it can limit only to the receiving-side equipment holding the encryption key information to which a communicative partner is transmitted by the 2nd means of communications. therefore, the physical relationship of mutual equipment is comparatively free -- etc. -- without spoiling the convenience of radio, informational secrecy nature can be held and the reliability on security can be secured

[0017] Invention according to claim 5 is set to communication system according to claim 4. the aforementioned transmitting-side equipment The same encryption key information as the encryption key information held at the aforementioned key information maintenance means When not held at the receiving key information maintenance means which the aforementioned receiving-side equipment has, it is characterized by having further a communication refusal means (for example, CPU21 which performs processing shown in Step S45 of drawing 5) to refuse transmission and reception of the radio signal by the 1st means of communications of the above.

[0018] When the same encryption key information as the encryption key information held at the key information maintenance means is not held at the receiving key information maintenance means which receiving-side equipment has, since transmission and reception of the radio signal by the 1st means of communications refuse, transmitting-side equipment can limit more the communication device which serves as a communicative partner to strictness, and, according to invention according to claim 5, can hold informational secrecy more certainly by the communication refusal means.

[0019] Invention according to claim 6 is characterized by the 2nd means of communications of the above which the aforementioned transmitting-side equipment has, and the key information receiving means which the aforementioned receiving-side equipment has transmitting [transmit and receive a radio signal by the communication mode to which the 1st means of communications which the aforementioned transmitting-side equipment has and the encryption information receiving means which the aforementioned receiving-side equipment has applied correspondingly to Bluetooth (Bluetooth) specification, and] and receiving a radio signal in communication system according to claim 4 or 5 by the communication mode which used an infrared signal.

[0020] According to invention according to claim 6, the 1st means of communications which transmitting-side equipment has, and the encryption information receiving means which receiving-side equipment has The 2nd means of communications which transmits and receives a radio signal by the communication mode according to the Bluetooth (Bluetooth) specification, and transmitting-side equipment has, With the key information receiving means which receiving-side equipment has, since a radio signal is transmitted and received by the communication mode using the infrared signal While specification is exhibited widely and it is rich in convenience, positive information secrecy can secure informational secrecy nature in the radio of the difficult Bluetooth (Bluetooth) specification. Since especially the 2nd means of communications and a key information receiving means use the communication mode which used the infrared signal, low-cost[the miniaturization of the 2nd means of communications and a key information receiving means, lightweight-izing, and]-izing and power-saving are possible for them, and they can be realized easily. Moreover, in the communication mode using the infrared signal, since transmitting-side equipment and receiving-side equipment need to

approach mutually and need to counter within a predetermined solid angle, they can raise informational secrecy nature further.
[0021] A key information transmission-control means by which the aforementioned transmitting-side equipment has invention according to claim 7 in communication system given in either of the claims 4-6 is characterized by enciphering the aforementioned encryption key information and making it transmit by the 2nd means of communications of the above.
[0022] According to invention according to claim 7, since encryption key information is enciphered and it is made to transmit by the 2nd means of communications, the key information transmission-control means which transmitting-side equipment has can prevent more certainly disclosure of the information at the time of transmitting encryption key information. Thereby, the reliability on security can be raised further.
[0023]
[Embodiments of the Invention] Hereafter, with reference to drawing, the gestalt of operation of this invention is explained in detail.
[0024] [Gestalt of the 1st operation] Drawing 1 is the block diagram showing the composition of the communication system 1 as a gestalt of the 1st operation which applied this invention. As shown in this drawing, communication system 1 is mutually constituted by the communication device 2 and communication device 3 which can communicate. Between a communication device 2 and a communication device 3, the radio link A through a radio electric wave and the infrared-ray-communication link B using infrared radiation are formed.
[0025] In addition, although the communication device 2 and communication device 3 which are shown in drawing 1 are a communication device which all becomes by the same composition, they explain the equipment of an access requestor side, and a communication device 3 for a communication device 2 as equipment of an access receiving side in the gestalt of operation of **** 1.
[0026] A communication device 2 is equipped with each part of CPU (Central Processing Unit)21, memory 22, the input section 23, the Radio Communications Department 24, an antenna 25, the infrared-ray-communication section 26, the infrared carrier luminescence unit 27, and the interface section 28, and is constituted.
[0027] CPU21 reads and performs the system program stored in memory 22 according to the directions operation in the input section 23, and carries out drive control of each part of a communication device 2. Specifically, according to the program in memory 22, CPU21 controls the Radio Communications Department 24, and establishes the radio link A between communication devices 3. Then, CPU21 establishes the infrared-ray-communication link B by the infrared-ray-communication section 26 and the infrared carrier luminescence unit 27. And CPU21 transmits the various information about the encryption stored in memory 22 to a communication device 3 through the infrared-ray-communication link B.
[0028] Then, CPU21 receives the information transmitted through the infrared-ray-communication link B from the communication device 3, checks the informational content, and cuts the radio link A between communication devices 3, and the infrared-ray-communication link B.
[0029] Moreover, CPU21 controls the Radio Communications Department 24, and makes the radio signal for carrying out the scan of the communication device which exists near a communication device 2 output from an antenna 25 according to the directions inputted from the input section 23. When a connectable communication device is detected through a radio circuit by this scanning operation, the information transmitted from the detected communication device is received and analyzed by the Radio Communications Department 24.
[0030] And the received information is collated with the primitive encryption information in which it was stored in memory 22, when in agreement, connection is permitted, and radio is started between the this detected communication devices. Moreover, when the received information is not in agreement with primitive encryption information, communication between these communication devices is refused.
[0031] Memory 22 is equipped with nonvolatile storage elements, such as EEPROM and a flash memory, and is constituted. Memory 22 stores the data concerning programs, such as a system program

performed by CPU21, and these programs etc. Moreover, memory 22 holds temporarily the data processed by CPU21, the data inputted from the input section 23.
[0032] Here, the data stored in memory 22 are explained. Drawing 2 is drawing showing the composition of the memory 22 interior typically. In memory 22, as shown in drawing 2 besides [which stored the various above-mentioned programs] a storing field (illustration abbreviation), the primitive encryption information storing field 101 and the transfer item information storing field 102 are formed.
[0033] Encryption key management information including the history which transmitted the encryption key information used as a "key" in the case of encryption and encryption key information to other electronic equipment is stored in the primitive encryption information storing field 101. The various information stored in the primitive encryption information storing field 101 is named primitive encryption information generically.
[0034] The primitive encryption information stored in this primitive encryption information storing field 101 is good also as what is beforehand stored in the primitive encryption information storing field 101, and may be made to be inputted by operation of the input section 23 at any time.
[0035] Moreover, various information, such as product information on a communication device 2, peculiar functional information, user information, and serial No., is stored in the transfer item information storing field 102. The various information stored in these transfer item information storing fields 102 is named transfer item information generically. In addition, the information stored in the transfer item information storing field 102 is good also as what is beforehand stored in memory 22, and good also as what is inputted by operation of the input section 23, or good also as what is inputted from the electronic equipment 4 connected to the interface section 28.
[0036] The input section 23 is equipped with input devices, such as two or more keys to which the information that it could input, respectively was assigned, generates the manipulate signal corresponding to the content of operation, and outputs it to CPU21.
[0037] The Radio Communications Department 24 builds in an encoder, a decoder, RF, amplifier, etc., changes the signal inputted from CPU21, generates a radio signal, and transmits to a communication device 3 through an antenna 25. Moreover, the Radio Communications Department 24 outputs the signal which receives the radio signal transmitted from the communication device 3 with an antenna 25, changes the radio signal which received, and is acquired to CPU21.
[0038] Here, as the Radio Communications Department 24, the radio unit according to the Bluetooth (Bluetooth) specification is mentioned, for example. Bluetooth specification is the radio specification upon which it was decided as the promotor constituted by two or more entrepreneurs who manufacture communication equipment, electronic equipment, software, etc. gathering by Bluetooth SIG (Special InterestGroup). By Bluetooth specification, radio is performed using the radio signal of the frequency of a 2.4GHz (G Hertz) band among two or more less than several [about] m electronic equipment.
[0039] The electronic equipment which carried the radio unit according to Bluetooth specification forms the group mutually called PIKONETSU. And it is possible to communicate mutually between the electronic equipment belonging to the same pico network. Many electronic equipment can belong to the same pico network simultaneously. Moreover, it is also possible for one set of a communication device to belong to two or more pico networks simultaneously. For this reason, carried type telephone is begun and it is observed as a communication mode which connects various devices of each other, such as a personal computer, a hand held computer called PDA (Personal Digital Assistant), a printer, and a music player. Hereafter, the Radio Communications Department 24 is a communication unit according to the above-mentioned Bluetooth specification, and explains the radio (radio through the radio link A) performed using the Radio Communications Department 24 and an antenna 25 as what is performed by the electric wave of the 2.4GHz band according to Bluetooth specification.
[0040] The infrared-ray-communication section 26 builds in the encoder, the decoder, etc., and is connected to the infrared carrier luminescence unit 27. The infrared-ray-communication section 26 changes the signal inputted from CPU21, and outputs it to the infrared carrier luminescence unit 27. The infrared carrier luminescence unit 27 makes Light Emitting Diode which builds in Light Emitting Diode (Light Emitting Diode), a photosensor, etc., and is built in based on the signal inputted from the

infrared-ray-communication section 26 emit light, and is outputted towards a communication device 3 as an infrared signal.

[0041] Moreover, if the infrared light from a communication device 3 is received with the photosensor to build in, the infrared carrier luminescence unit 27 will change a light-receiving pattern into a predetermined signal, and will output it to the infrared-ray-communication section 26. Furthermore, the infrared-ray-communication section 26 changes the signal inputted from the infrared carrier luminescence unit 27, and outputs it to CPU21.

[0042] The interface section 28 is an interface for connecting a communication device 2 and the electronic equipment of the exterior of a communication device 2, and is equipped with the connector etc. Here, as electronic equipment 5 connected to the interface section 28, although carried type telephone, a personal computer, PDA, etc. are mentioned, it is not limited especially, for example. Moreover, although a communication device 2 builds in rechargeable batteries, such as a lithium ion battery which is not illustrated and a nickel-cadmium battery, or a dry cell and operates considering these cells as a power supply, it is good also as composition in which a power supply is supplied to a communication device 2 through the interface section 28 to a communication device 2, without building in a cell.

[0043] Furthermore, it is good also as composition using the input unit which the device which replaced with the input section 23 which a communication device 2 has, and was connected to the interface section 28 possesses. In this case, CPU21 does not need to be equipped with the input section 23 that what is necessary is just to operate according to the signal inputted from the device connected to the interface section 28.

[0044] Subsequently, the composition of a communication device 3 is explained. A communication device 3 is equipped with each part of CPU31, memory 32, the input section 33, the Radio Communications Department 34, an antenna 35, the infrared-ray-communication section 36, the infrared carrier luminescence unit 37, and the interface section 38, and is constituted. Here, each part of the above-mentioned memory 32, the input section 33, the Radio Communications Department 34, an antenna 35, the infrared-ray-communication section 36, the infrared carrier luminescence unit 37, and the interface section 38 becomes by the same composition as each part of the memory 22 which a communication device 2 has, the input section 23, the Radio Communications Department 24, an antenna 25, the infrared-ray-communication section 26, the infrared carrier luminescence unit 27, and the interface section 28, and omits explanation.

[0045] CPU31 reads and performs the system program stored in memory 32 according to the directions operation in the input section 33, and carries out drive control of each part of a communication device 3. Specifically, according to the program in memory 32, CPU31 controls the Radio Communications Department 34, and establishes the radio link A between communication devices 2.

[0046] Then, CPU31 establishes the infrared-ray-communication link B by the infrared-ray-communication section 36 and the infrared carrier luminescence unit 37. And CPU31 receives the infrared signal emitted from the infrared carrier luminescence unit 27 which a communication device 2 has by the infrared carrier luminescence unit 37, and receives the various information about the encryption transmitted from the communication device 2.

[0047] Here, CPU31 transmits this information to a communication device 2 through the infrared-ray-communication section 36 and the infrared carrier luminescence unit 37 while storing the various information transmitted from the communication device 2 in memory 32. And when the radio signal outputted from the antenna 25 which a communication device 2 has is received and the received signal is demanding cutting of the radio link A and the infrared-ray-communication link B, the radio link A between communication devices 2 and the infrared-ray-communication link B are cut.

[0048] Next, operation of the gestalt of this operation is explained. Drawing 3 is a flow chart which shows operation of the communication system 1 in the gestalt of operation of **** 1. Drawing 3 (a) shows operation of the equipment 2 of an access requestor side, i.e., a communication device, and drawing 3 (b) shows operation of the equipment 3 of an access receiving side, i.e., a communication device. In addition, the signal shown by the solid line arrow is a radio signal according to the above-

mentioned Bluetooth specification transmitted and received through the radio link A (drawing 1) among drawing, and the signal shown by the dashed line arrow is an infrared signal transmitted and received through the infrared-ray-communication link B (drawing 1).
[0049] First, CPU21 starts operation according to the directions input from the input section 23, generates the connection-request signal which asks for connection from a communication device 3, and is made to transmit it to a communication device 3 by the Radio Communications Department 24, as shown in drawing 3 (a) (Step S11).
[0050] CPU31 starts operation by the directions input from the input section 33, and shifts to the state where the radio signal transmitted by the Radio Communications Department 34 from a communication device 2 is receivable. And when the Radio Communications Department 34 receives the connection request transmitted from the Radio Communications Department 24 (Step S21), the connection-confirm signal used as the check of connection is generated, and it is made to transmit by the Radio Communications Department 34 (Step S22).
[0051] When the Radio Communications Department 24 receives the connection-confirm signal transmitted from the Radio Communications Department 34 by control of CPU31 (Step S12), CPU21 reads the transfer item information stored in the transfer item information storing field 102 of memory 22, and is made to transmit it to a communication device 3 as an infrared signal by the infrared-ray-communication section 26 and the infrared carrier luminescence unit 27 (Step S13).
[0052] When the infrared-ray-communication section 36 receives the transfer item information transmitted by the infrared-ray-communication section 26 of a communication device 2 as an infrared signal (Step S23), CPU31 reads the transfer item information stored in the transfer item information storing field 102 of memory 32, and is made to transmit it by the infrared-ray-communication section 36 (Step S24).
[0053] When the infrared-ray-communication section 26 receives the transfer item information transmitted from the communication device 3 (Step S14), CPU21 reads the primitive encryption information stored in the primitive encryption information storing field 101 in memory 22, and is made to transmit it to a communication device 3 by the infrared-ray-communication section 26 (Step S15).
[0054] CPU31 makes the primitive encryption information storing field 101 in memory 32 memorize received primitive encryption information, when the primitive encryption information transmitted from the communication device 2 is received (Step S25) (Step S26). In addition, about the primitive encryption information beforehand stored in the primitive encryption information storing field 101 of memory 32, it is good also as what is overwritten by the newly received primitive encryption information, or is good here also as what is saved to a different field from the newly received primitive encryption information.
[0055] Then, CPU31 is received at Step S25, and the primitive encryption information memorized to the primitive encryption information storing field 101 in memory 32 is transmitted to a communication device 2 by the infrared-ray-communication section 36 (Step S27).
[0056] It checks that CPU21 collates the received primitive encryption information and the primitive encryption information stored in the primitive encryption information storing field 101 of memory 22, and is in agreement if the primitive encryption information transmitted from the communication device 3 is received (Step S16) (Step S17). That is, it is checked that transmission and reception of the encryption information in Steps S15, S16, S25, and S26 have been performed satisfactory by checking that the primitive encryption information transmitted to the communication device 3 at Step S15 and the primitive encryption information transmitted from the communication device 3 are in agreement.
[0057] And CPU21 generates the disconnect-request signal which requires communicative cutting, and is made to transmit it to a communication device 3 by the Radio Communications Department 24 (Step S18). If the Radio Communications Department 34 receives the disconnect-request signal transmitted from the communication device 2 (Step S28), CPU31 generates the disconnect-confirm signal which checks reception of a disconnect request, and by the Radio Communications Department 34, it will be made to transmit to a communication device 2 (Step S29), and it will end this processing.
[0058] Moreover, CPU21 will end this processing, if the Radio Communications Department 24

receives the disconnect-confirm signal transmitted from the communication device 3 (Step S19).
[0059] By processing shown in the above drawing 3 , the primitive encryption information beforehand stored in the primitive encryption information storing field 101 in memory 22 will be stored the memory 22 which a communication device 2 has, and the memory 32 which a communication device 3 has.
[0060] In the processing shown in drawing 3 , transfer item information and primitive encryption information are transmitted and received through the infrared-ray-communication link B (drawing 1). Generally, when performing radio by the infrared signal, it is required for the infrared carrier light-emitting part which the electronic equipment which communicates is mutually close, and mutual electronic equipment has to have countered. Possibility of especially the infrared carrier light-emitting part that mutual electronic equipment has must counter so that it may fit in a comparatively narrow solid angle, and being monitored by unrelated electronic equipment is low, and the concern on security is small. However, let reliability on the security in communication through the infrared-ray-communication link B be a more positive thing by giving encryption described below.
[0061] In drawing 4 (a), the hierarchical model which shows the protocol composition in the infrared ray communication at the time of enciphering is illustrated. Moreover, the composition of the data unit in infrared ray communication is typically shown in drawing 4 (b).
[0062] If the compatibility in a data link layer, a link management layer, and a transport layer is held in infrared ray communication, protocol compatibility can be kept general even if it enciphers the service data unit in the hierarchy of a high order from it. Therefore, as shown in drawing 4 (a), the layer of a high order is used as an encryption layer rather than a transport layer, and the secrecy nature of the information transmitted can be maintained further, maintaining the security data-exchange protocol layer which exchanges above-mentioned transfer item information and above-mentioned primitive encryption information for the high order layer, then protocol compatibility.
[0063] What is necessary is just to specifically, encipher the service data unit following the Protocol Data Unit of leucine aminopeptidase (data link layer), LMP (link management layer), and TP (transport layer), as shown in drawing 4 (b). Therefore, let secrecy nature of transfer item information or primitive encryption information transmitted and received by the processing shown in drawing 3 be a more positive thing in the both sides of a communication device 2 and a communication device 3 by performing the encryption and the decode of a signal which are transmitted and received through the infrared-ray-communication link B.
[0064] Drawing 5 is a flow chart which shows operation of the communication device 2 after execution of the processing shown in drawing 3 . In the processing shown in this drawing 5 , a communication device 2 operates as a device of Master specified by Bluetooth specification. Moreover, the radio signal transmitted and received in the processing shown in drawing 5 is a radio signal of the 2.4GHz band according to Bluetooth specification.
[0065] First, CPU21 starts operation according to the directions inputted from the input section 23, the Radio Communications Department 24 is controlled, Page Scan operation is performed, and the communication device in which communication according to Bluetooth specification is possible is detected (Step S41).
[0066] And when a connectable communication device is detected, the information transmitted from the equipment detected according to Page Scan operation by CPU21 is received (Step S42), and collating with the received information and the primitive encryption information stored in the primitive encryption information storing field 101 in memory 22 is performed (Step S43).
[0067] Here, when a communication device 2 detects a communication device 3, since the communication device 3 has already held the primitive encryption information stored in the primitive encryption information storing field 101 in memory 22, it transmits the information enciphered according to primitive encryption information according to Page Scan operation. Moreover, when a communication device with unrelated communication device 2 and communication device 3 is detected, from this unrelated communication device, the usual radio signal is transmitted according to Page Scan operation. Therefore, it can distinguish whether the communication device detected at Step S41 is a communication device 3 by collating in Step S43.

[0068] As a result of collating in Step S43, when the radio signal which received at Step S42 is to primitive encryption information, (Step S44; No) and CPU21 refuse connection with the detected communication device (Step S45), and end this processing.
[0069] Moreover, when the radio signal which received at Step S42 suits primitive encryption information by collating at Step S43, (Step S44; Yes) and CPU21 start transmission and reception of the radio signal enciphered by the primitive encryption information in the primitive encryption information storing field 101 between the detected communication devices (Step S46). In addition, the information enciphered by the primitive encryption information stored in the primitive encryption information storing field 101 can be decoded based on this primitive encryption information. For this reason, while CPU21 enciphers the information transmitted by the Radio Communications Department 24, it decodes the information received by the Radio Communications Department 24.
[0070] And CPU21 permits use with application, after the negotiation between the detected communication devices is completed (Step S47). Then, CPU21 performs processing which transmits receives the enciphered radio signal according to the demand of the application program performed on the electronic equipment 4 connected to a communication device 2 or the interface section 28 (Step S48), and ends this processing by the directions input from the input section 23.
[0071] As mentioned above, the Radio Communications Department 24 and the antenna 25 which perform radio according to Bluetooth specification according to the gestalt of operation of the 1st of this invention, In between the communication device 2 equipped with the infrared-ray-communication section 26 and the infrared carrier luminescence unit 27 which perform radio using the infrared signal, and communication devices 2 and the communication devices 3 which become by the same composition Beforehand, primitive encryption information is transmitted by infrared ray communication, and it transmits the information enciphered based on the transmitted primitive encryption information and receives by the radio according to Bluetooth specification after that. While this maintains high secrecy nature, high communication of the convenience according to Bluetooth specification can be performed.
[0072] That is, when the radio according to Bluetooth specification is used, a pico network is formed only by making a mutual communication device approach, and communication can be started. Moreover, each communication equipment under communication can form a pico network among other communication devices simultaneously, and can perform flexible communication. Furthermore, the communication device which forms a pico network has that a position is restrained [little] that what is necessary is just close within a predetermined distance mutually. On the other hand, in the radio according to Bluetooth specification, it is difficult to transmit information only to a specific communication device, and possibility of being accidentally received by the unrelated communication device cannot be denied. However, it transmits [according to the communication system 1 in the gestalt of implementation of the above 1st, / primitive encryption information is shared without being influenced by the unrelated communication device, and] the information enciphered using this primitive encryption information and receives by the radio according to Bluetooth specification beforehand by transmitting primitive encryption information by infrared ray communication between a communication device 2 and a communication device 3. Therefore, high radio of convenience can be performed, securing the reliability on security.
[0073] In addition, in the form of the above-mentioned implementation, although radio shall be performed through the radio link A according to Bluetooth specification, it is not limited to this, and specification and specification are exhibited, or this invention can be applied also to the radio method with which it spreads widely and compatibility is maintained, and, as for a communication device 2 and a communication device 3, does so the same effect as the above-mentioned communication system 1.
[0074] Furthermore, when applying this invention to various electronic equipment, such as carried type telephone, PDA and a personal computer, a printer, and a music player, of course, it is possible to also make the function of communication devices 2 and 3 build not only in composition but in the various above-mentioned electronic equipment to which electronic equipment 4 and 5 is connected to a communication device 2 and a communication device 3 as shown in drawing 1 .
[0075] Moreover, in the gestalt of implementation of the above 1st, although the processing which the

communication device 2 and the communication device 3 all possess the input sections 23 and 33, and is shown in drawing 3 by the directions input in these input sections 23 and 33 shall be started, you may not necessarily be composition equipped with the input sections 23 and 33. Hereafter, this case is explained as a gestalt of the 2nd operation.

[0076] [Gestalt of the 2nd operation] Drawing 6 is the block diagram showing the composition of the communication system 10 in the gestalt of operation of the 2nd of this invention.

[0077] As shown in this drawing, communication system 10 is constituted by a communication device 2 and communication device 3a. If communication system 10 removes the memory 61 and the switch 62 which communication device 3a has, it becomes by the same composition as the communication system 1 in the gestalt of implementation of the above 1st, attaches a same sign about an intersection, and omits explanation.

[0078] Whenever the switch 62 is equipped with one piece or two or more switches and is operated, it generates a manipulate signal and outputs it to CPU31.

[0079] Drawing 7 is drawing showing the internal configuration of memory 61 typically. As shown in this drawing, in memory 61, the primitive encryption information storing field 103 and the transfer item information storing field 102 are formed, and transfer item information, such as product information, peculiar functional information, user information, and serial No., is stored in the transfer item information storing field 102. On the other hand, primitive encryption information is not stored in the primitive encryption information storing field 103 in advance.

[0080] In the communication system 1 explained with the gestalt of implementation of the above 1st, in the processing shown in drawing 3 , primitive encryption information is transmitted to a communication device 3 from a communication device 2, and the primitive encryption information stored in the primitive encryption information storing field 101 of memory 22 is stored in the primitive encryption information storing field 101 of memory 32. In the communication system 10 in the gestalt of operation of **** 2, when primitive encryption information is transmitted to communication device 3a from a communication device 2, the transmitted primitive encryption information is stored in the primitive encryption information storing field 103 of memory 61. Therefore, communication device 3a can operate like the above-mentioned communication device 3.

[0081] Moreover, the processing shown in drawing 3 shall be started in the communication system 1 explained with the gestalt of implementation of the above 1st by the directions input in the input section 33 which the input section 23 and the communication device 3 which a communication device 2 has have. In the communication system 10 in the gestalt of operation of **** 2, processing shown in drawing 3 and same processing are performed by the directions input in the input section 23 which a communication device 2 has, and switch operation of the switch 62 which communication device 3a has.

[0082] That is, although communication device 3a is equipment equipped only with a switch 62 as an input means, it is usable as equipment which performs only operation which replaces with the communication device 3 in the gestalt of implementation of the above 1st, and receives access by the communication device 2. Moreover, since it replaces with a communication device 2 and does not use as equipment of an access requestor side, it is not necessary to store primitive encryption information in the primitive encryption information storing field 103 of memory 61 beforehand.

[0083] Therefore, the communication system 10 in the gestalt of operation of **** 2 does so the same effect as the gestalt of implementation of the above 1st using communication device 3a which has only the input switch 62. Thereby, the equipment which functions only as a device of Slave in the radio according to Bluetooth specification can only be equipped with a mere switch as an input means, and the same effect as communication system 1 can be acquired to it.

[0084]

[Effect of the Invention] According to the communication device of invention according to claim 1, the information transmitted serves as ready-for-receiving ability only by the communication device which received the encryption key information transmitted by the 2nd means of communications. Thereby, the reliability on security is securable about the radio by the 1st means of communications. Especially when

the radio by the 1st means of communications applies to the radio method with which specification and specification are exhibited, or it spreads widely like for example, the Bluetooth specification, and compatibility is maintained correspondingly, possibility of being received by the unrelated communication device cannot be denied. However, if this invention is applied, it can limit only to the communication device which received the encryption key information to which a communicative partner is transmitted by the 2nd means of communications. therefore, physical relationship with the equipment of a communications partner is comparatively free -- etc. -- without spoiling the convenience of radio, informational secrecy nature can be held and the reliability on security can be secured

[0085] According to the communication device of invention according to claim 2, the communication device which serves as a communicative partner since transmission and reception of the radio signal according to the 1st means of communications by the communication refusal means to the external communication device which does not hold the same encryption key information as the encryption key information held at the key information maintenance means are refused can be limited strictly, and informational secrecy can be held more certainly.

[0086] While according to the communication device of invention according to claim 3 specification is exhibited widely and it is rich in convenience, positive information secrecy can secure informational secrecy nature in the radio of the difficult Bluetooth (Bluetooth) specification. Since the communication mode which used the infrared signal for the 2nd means of communications especially is used, the 2nd low-cost[the miniaturization of means of communications, lightweight-izing, and]-izing and power-saving are possible, and it can realize easily. Moreover, in the communication mode using the infrared signal, since a communication device needs to approach mutually and it is necessary to counter within a predetermined solid angle, informational secrecy nature can be raised further.

[0087] According to the communication system of invention according to claim 4, and the correspondence procedure of invention according to claim 8, the information transmitted by transmitting-side equipment is receivable with receiving-side equipment. Thereby, the reliability on security is securable about the radio in the communication system using the 1st means of communications which transmitting-side equipment has. Especially when the radio by the 1st means of communications applies to the radio method with which specification and specification are exhibited, or it spreads widely like for example, the Bluetooth specification, and compatibility is maintained correspondingly, possibility of being received by the unrelated communication device cannot be denied. However, if this invention is applied, it can limit only to the receiving-side equipment holding the encryption key information to which a communicative partner is transmitted by the 2nd means of communications. therefore, the physical relationship of mutual equipment is comparatively free -- etc. -- without spoiling the convenience of radio, informational secrecy nature can be held and the reliability on security can be secured

[0088] When the same encryption key information as the encryption key information held at the key information maintenance means is not held at the receiving key information maintenance means which receiving-side equipment has, since transmission and reception of the radio signal by the 1st means of communications refuse, transmitting-side equipment can limit more the communication device which serves as a communicative partner to strictness, and, according to the communication system of invention according to claim 5, can hold informational secrecy more certainly by the communication refusal means.

[0089] While according to the communication system of invention according to claim 6 specification is exhibited widely and it is rich in convenience, positive information secrecy can secure informational secrecy nature in the radio of the difficult Bluetooth (Bluetooth) specification. Since especially the 2nd means of communications and a key information receiving means use the communication mode which used the infrared signal, low-cost[the miniaturization of the 2nd means of communications and a key information receiving means, lightweight-izing, and]-izing and power-saving are possible for them, and they can be realized easily. Moreover, in the communication mode using the infrared signal, since transmitting-side equipment and receiving-side equipment need to approach mutually and need to counter within a predetermined solid angle, they can raise informational secrecy nature further.

[0090] According to the communication system of invention according to claim 7, since encryption key information is enciphered and it is made to transmit by the 2nd means of communications, the key information transmission-control means which transmitting-side equipment has can prevent more certainly disclosure of the information at the time of transmitting encryption key information. Thereby, the reliability on security can be raised further.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the composition of the communication system 1 in the gestalt of the 1st operation which applied this invention.
[Drawing 2] It is drawing showing typically the internal configuration of the memory 22 and 32 of drawing 1 .
[Drawing 3] It is the flow chart which shows operation of the communication system 1 of drawing 1 , and (a) shows operation of a communication device 2 and (b) shows operation of a communication device 3.
[Drawing 4] It is explanatory drawing showing the protocol composition at the time of enciphering to the processing shown in drawing 3 , and (a) shows the hierarchical model which shows the protocol composition in the infrared ray communication at the time of enciphering, and (b) shows typically the composition of the data unit in infrared ray communication.
[Drawing 5] It is the flow chart which shows operation at the time of performing radio which applied to Bluetooth specification correspondingly by the communication device 2 of drawing 1 .
[Drawing 6] It is the block diagram showing the composition of the communication system 10 in the gestalt of the 2nd operation which applied this invention.
[Drawing 7] It is drawing showing typically the internal configuration of the memory 61 shown in drawing 6 .
[Description of Notations]
1 Ten Communication system
2 Three Communication device
21,31 CPU
22 32 Memory
23 33 Input section
24 34 Radio Communications Department
25 35 Antenna
26 36 Infrared-ray-communication section
27 37 Infrared carrier luminescence unit
28 38 Interface section
61 Memory
62 Switch
101,103 Primitive encryption information storing field
102 Transfer Item Information Storing Field

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The communication device characterized by providing the following The 1st means of communications which transmits and receives a radio signal The 2nd means of communications which transmits and receives a signal by different communication mode from this 1st means of communications A key information maintenance means to hold encryption key information A key information transmission-control means to make the encryption key information held at this key information maintenance means transmit to other communication devices by the 2nd means of communications of the above, and the communications control means to which encipher information based on the encryption key information held at the aforementioned key information maintenance means, and it is made to transmit by the 1st means of communications of the above
[Claim 2] The communication device according to claim 1 characterized by having further a communication refusal means to refuse transmission and reception of the radio signal by the 1st means of communications of the above, to the external communication device which does not hold the same encryption key information as the encryption key information held at the aforementioned key information maintenance means.
[Claim 3] It is the communication device according to claim 1 or 2 characterized by for the 1st means of communications of the above transmitting and receiving a radio signal by the communication mode according to the Bluetooth specification, and the 2nd means of communications of the above transmitting and receiving a radio signal by the communication mode which used the infrared signal.
[Claim 4] It is the communication system which comes to have transmitting-side equipment and receiving-side equipment. the aforementioned transmitting-side equipment The 1st means of communications which transmits and receives a radio signal, and the 2nd means of communications which transmit and receive a signal by different communication mode from this 1st means of communications, A key information maintenance means to hold encryption key information, and a key information transmission-control means to make the encryption key information held at this key information maintenance means transmit to the aforementioned receiving-side equipment by the 2nd means of communications of the above, Information is enciphered based on the encryption key information held at the aforementioned key information maintenance means, and it has the communications control means made to transmit to the aforementioned receiving-side equipment by the 1st means of communications of the above. the aforementioned receiving-side equipment A key information receiving means to receive the encryption key information transmitted by the 2nd means of communications which the aforementioned transmitting-side equipment has, Communication system characterized by having a receiving key information maintenance means to hold the encryption key information received by this key information receiving means, and an encryption information receiving means to receive the information transmitted by the 1st means of communications which the aforementioned transmitting-side equipment has.
[Claim 5] The aforementioned transmitting-side equipment is communication system according to claim 4 characterized by to have further a communication refusal means refuse transmission and reception of

the radio signal by the 1st means of communications of the above when the same encryption key information as the encryption key information held at the aforementioned key information maintenance means is not held at the receiving key information maintenance means which the aforementioned receiving-side equipment has.

[Claim 6] For the 1st means of communications which the aforementioned transmitting-side equipment has, and the encryption information receiving means which the aforementioned receiving-side equipment has, the 2nd means of communications of the above which transmits and receives a radio signal by the communication mode according to the Bluetooth specification, and the aforementioned transmitting-side equipment has, and the key information receiving means which the aforementioned receiving-side equipment has are the communication system according to claim 4 or 5 characterized by to transmit and receive a radio signal by the communication mode which used the infrared signal.

[Claim 7] The key information transmission-control means which the aforementioned transmitting-side equipment has is communication system given in either of the claims 4-6 characterized by enciphering the aforementioned encryption key information and making it transmit by the 2nd means of communications of the above.

[Claim 8] The 1st means of communications which transmits and receives a radio signal The 2nd means of communications which transmits and receives a signal by different communication mode from this 1st means of communications Are the correspondence procedure equipped with the above and with the process which transmits encryption key information to the aforementioned receiving-side equipment by the 2nd means of communications of the above with the aforementioned transmitting-side equipment, and the aforementioned receiving-side equipment It is characterized by including the process which receives and memorizes the encryption key information transmitted by the 2nd means of communications which the aforementioned transmitting-side equipment has, and the process which enciphers information based on the aforementioned encryption key information with the aforementioned transmitting-side equipment, and is transmitted to the aforementioned receiving-side equipment by the 1st means of communications of the above.

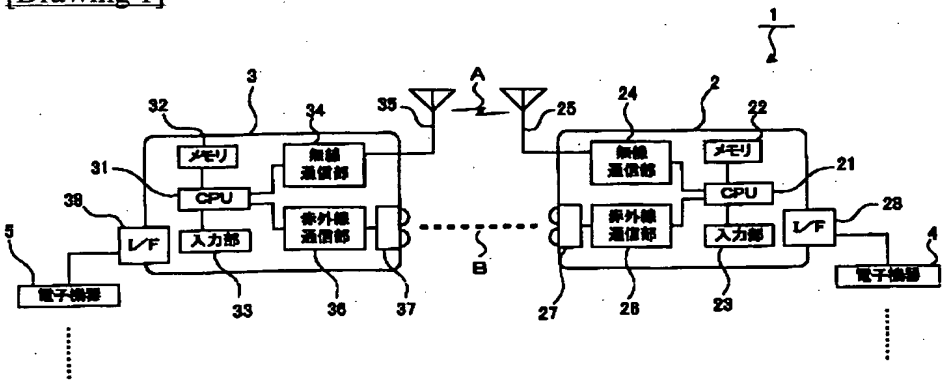
[Translation done.]

* NOTICES *

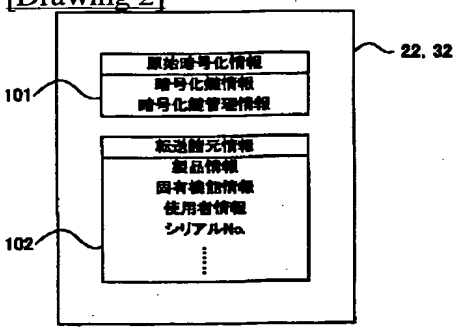
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]

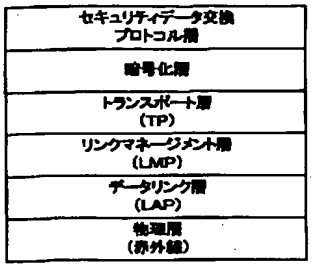


[Drawing 2]

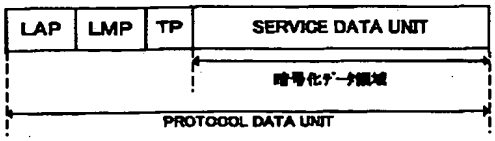


[Drawing 4]

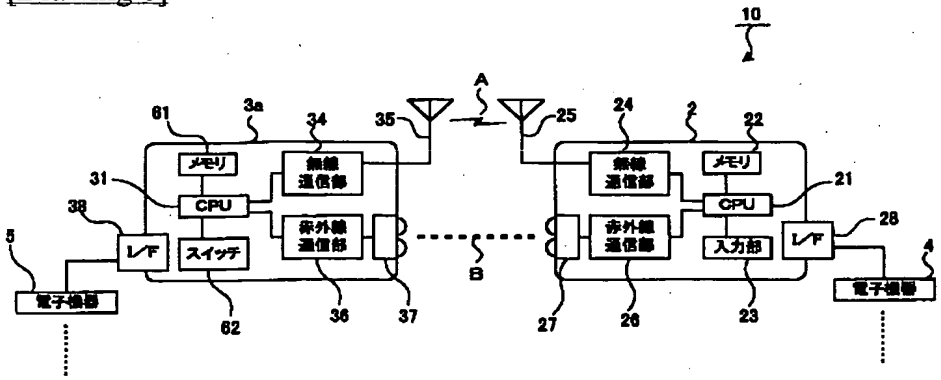
(a)



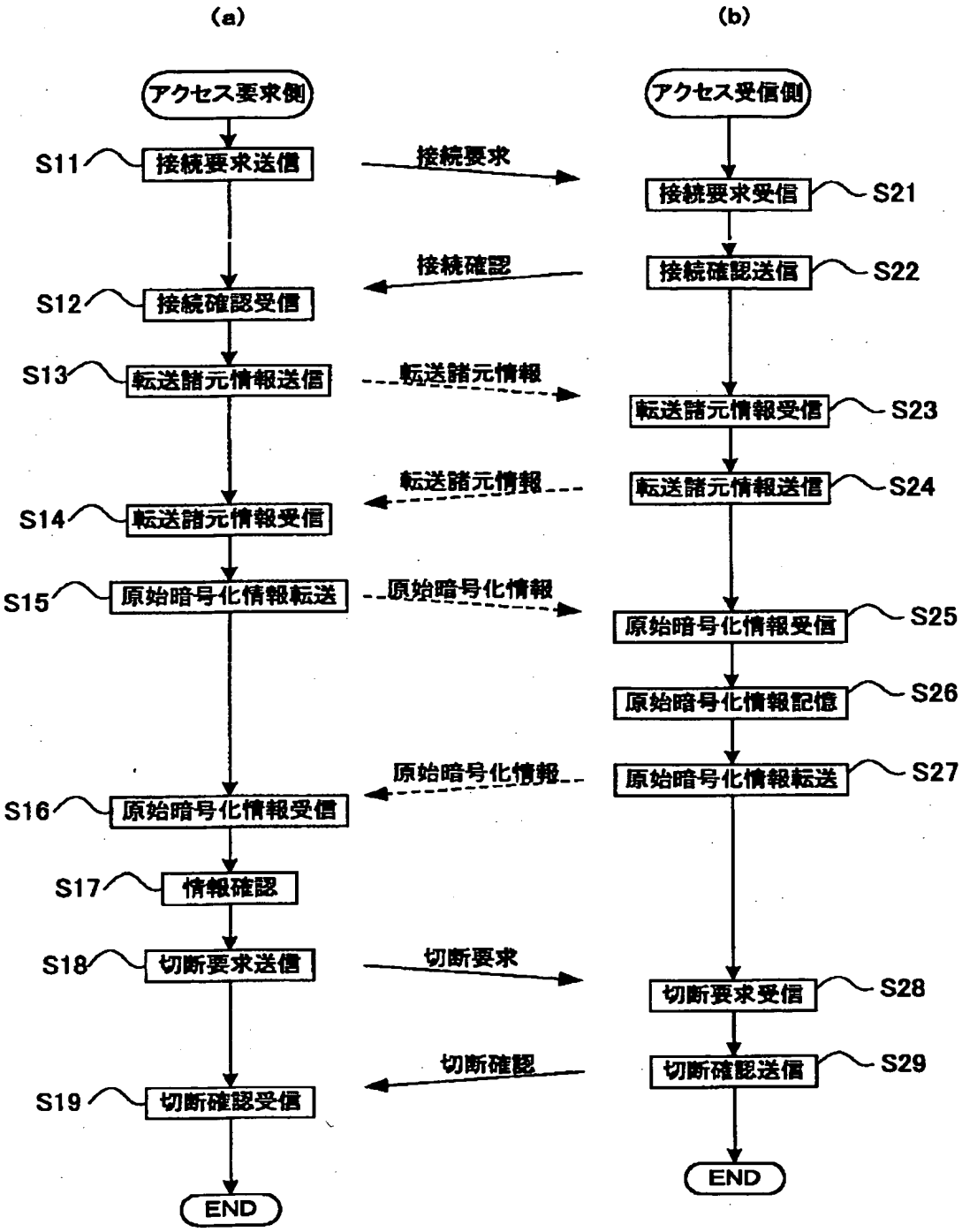
(b)



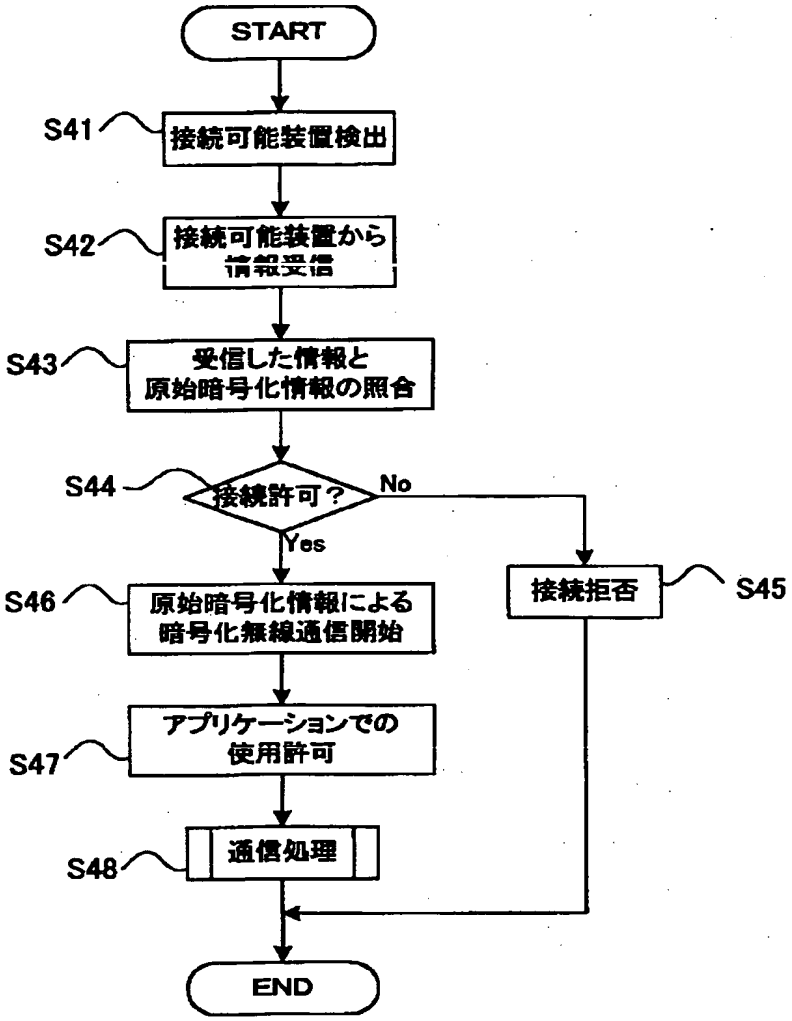
[Drawing 6]



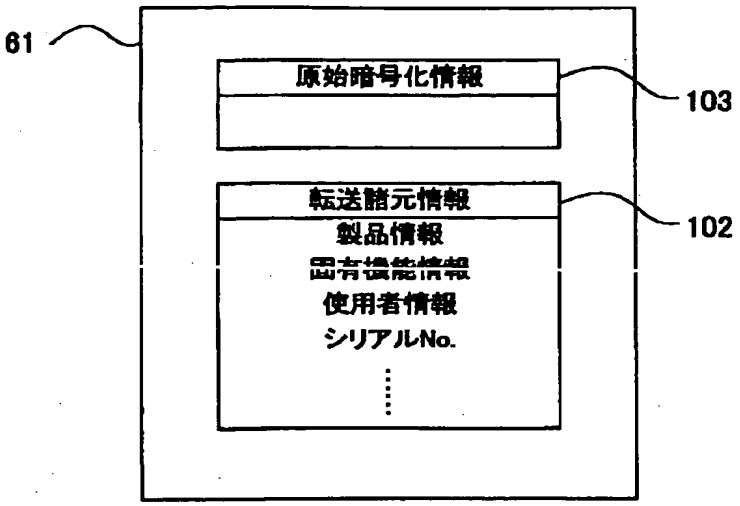
[Drawing 3]


(a)
(b)
アクセス要求側
アクセス受信側
S11
接続要求送信
接続要求
接続要求受信
S21
接続確認
接続確認送信
S22
S12
接続確認受信
S13
転送諸元情報送信
転送諸元情報
転送諸元情報受信
S23
転送諸元情報
転送諸元情報送信
S24
S14
転送諸元情報受信
S15
原始暗号化情報転送
原始暗号化情報
原始暗号化情報受信
S25
原始暗号化情報記憶
S26
原始暗号化情報
原始暗号化情報転送
S27
S16
原始暗号化情報受信
S17
情報確認
S18
切断要求送信
切断要求
切断要求受信
S28
切断確認
切断確認送信
S29
S19
切断確認受信
END
END

[Drawing 5]


START
S41
接続可能装置検出
S42
接続可能装置から
情報受信
S43
受信した情報と
原始暗号化情報の照合
S44
接続許可？
No
Yes
S45
接続拒否
S46
原始暗号化情報による
暗号化無線通信開始
S47
アプリケーションでの
使用許可
S48
通信処理
END

[Drawing 7]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－124960
（P2002－124960A）
(43)公開日　平成14年４月26日(2002.4.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｂ	５Ｊ１０４
9/08		9/00	６０１Ｃ	５Ｋ０３３

審査請求　未請求　請求項の数８　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－315395(P2000－315395)

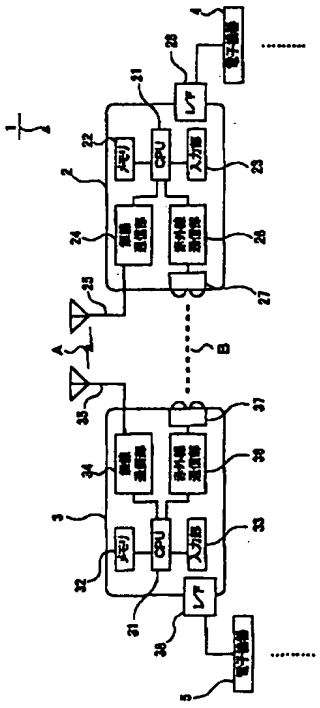
(22)出願日　平成12年10月16日(2000.10.16)

(71)出願人　500225837
リンク・エボリューション株式会社
東京都世田谷区松原３丁目40番７号
(72)発明者　北角　権太郎
東京都世田谷区松原３丁目40番７号　リンク・エボリューション株式会社内
(74)代理人　100090033
弁理士　荒船　博司　（外１名）

Ｆターム(参考)　5J104 AA16 EA04 EA21 NA02 NA37
5K033 AA08 CB06 DA17 DA20

(54)【発明の名称】　通信装置、通信システム、及び、通信方法

(57)【要約】
【課題】　複数の電子機器間で無線通信によってデータを送受信する場合に、無線通信の利便性を損なうことなくセキュリティ上の信頼性を向上させる。
【解決手段】　通信装置２と通信装置３との間において、Bluetooth規格に準じた無線通信リンクＡと、赤外線通信リンクＢとを介してデータを送受信する通信システム１であって、通信装置２は、メモリ２２内に保持する原始暗号化情報を、赤外線通信リンクＢを介して通信装置３へ送信し、通信装置３は、送信された原始暗号化情報を受信してメモリ３２内に保持する。そして、通信装置２から通信装置３へ無線通信リンクＡを介して情報を送信する場合は、メモリ２２内の原始暗号化情報に基づいて暗号化した情報を送信する。



1

【特許請求の範囲】

【請求項１】無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段と、

暗号化鍵情報を保持する鍵情報保持手段と、

この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって他の通信装置へ送信させる鍵情報送信制御手段と、

前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって送信させる通信制御手段と、

を備えることを特徴とする通信装置。

【請求項２】前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、前記第１の通信手段による無線信号の送受信を拒否する通信拒否手段をさらに備えることを特徴とする請求項１記載の通信装置。

【請求項３】前記第１の通信手段はブルートゥース規格に準じた通信方式により無線信号を送受信するものであって、

前記第２の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする請求項１または２記載の通信装置。

【請求項４】送信側装置と受信側装置とを備えてなる通信システムであって、

前記送信側装置は、

無線信号を送受信する第１の通信手段と、

この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段と、

暗号化鍵情報を保持する鍵情報保持手段と、

この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって前記受信側装置へ送信させる鍵情報送信制御手段と、

前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって前記受信側装置へ送信させる通信制御手段とを備え、前記受信側装置は、

前記送信側装置が有する第２の通信手段により送信された暗号化鍵情報を受信する鍵情報受信手段と、

この鍵情報受信手段により受信された暗号化鍵情報を保持する受信鍵情報保持手段と、

前記送信側装置が有する第１の通信手段により送信された情報を受信する暗号化情報受信手段とを備えること、

を特徴とする通信システム。

【請求項５】前記送信側装置は、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、前記受信側装置が有する受信鍵情報保持手段に保持されていない場合に、前記第１の通信手段による無線信号の送受信を拒否する通信拒否手段をさらに備えることを特徴とする請求項４記載の通信システム。

2

【請求項６】前記送信側装置が有する第１の通信手段と、前記受信側装置が有する暗号化情報受信手段とは、ブルートゥース規格に準じた通信方式により無線信号を送受信するものであって、

前記送信側装置が有する前記第２の通信手段と、前記受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする請求項４または５記載の通信システム。

【請求項７】前記送信側装置が有する鍵情報送信制御手段は、前記暗号化鍵情報を暗号化して前記第２の通信手段によって送信させることを特徴とする請求項４から６のいずれかに記載の通信システム。

【請求項８】無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段とを有する送信側装置と、受信側装置とを備えてなる通信システムにおける通信方法であって、

前記送信側装置により、暗号化鍵情報を前記第２の通信手段によって前記受信側装置へ送信する工程と、

前記受信側装置により、前記送信側装置が有する第２の通信手段により送信された暗号化鍵情報を受信して記憶する工程と、

前記送信側装置により、前記暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって前記受信側装置へ送信する工程と、

を含むことを特徴とする通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、異なる複数の通信方式に対応する通信装置、この通信装置を備える通信システム、及び、この通信システムにおける通信方法に関する。

【０００２】

【従来の技術】従来、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant）、携帯電話機等の電子機器間でデータ通信を行う場合には、互いの電子機器をケーブルで接続する手法が用いられていた。しかし、ケーブルを用いた手法は、電子機器にケーブルを接続する手間がかかり、ケーブルを携帯しなければならないため、不便であった。そこで、最近では、複数の電子機器間におけるデータ通信に無線通信技術が用いられるようになった。

【０００３】特に、近年では、電子機器の利便性を向上させるため、互換性に富む複数の無線通信規格が策定されている。これらの通信規格に準じた通信装置を用いれば、様々な電子機器との間でデータ通信を容易に行うことができる。

【０００４】

【発明が解決しようとする課題】しかしながら、無線通信技術を利用してデータ通信を行う場合は、データの漏

3

洩に注意する必要があった。特に、様々な機器との間で通信可能な通信規格に準じている場合は、誤って無関係な他の機器によってデータが受信されないように注意する必要があった。このように、無線通信技術を用いたデータ通信では、セキュリティ上の信頼性を向上することが課題となっていた。

【０００５】本発明の課題は、複数の電子機器間で無線通信によってデータを送受信する場合に、無線通信の利便性を損なうことなくセキュリティ上の信頼性を向上させることである。

【０００６】

【課題を解決するための手段】本発明は、このような課題を解決するために、次のような特徴を備えている。なお、次に示す手段の説明中、括弧書きにより実施の形態に対応する構成を一例として示す。符号等は、後述する図面参照符号等である。

【０００７】請求項１記載の発明の通信装置（２）は、無線信号を送受信する第１の通信手段（例えば、図１に示す無線通信部２４）と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段（例えば、図１に示す赤外線通信部２６）と、暗号化鍵情報を保持する鍵情報保持手段（例えば、図２に示す原始暗号化情報格納領域１０１を有するメモリ２２）と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって他の通信装置へ送信させる鍵情報送信制御手段（例えば、図３（ａ）に示す処理を行うＣＰＵ２１）と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって送信させる通信制御手段（例えば、図５に示す処理を行うＣＰＵ２１）とを備えることを特徴とする。

【０００８】この請求項１記載の発明によれば、無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段とを備え、鍵情報保持手段により、暗号化鍵情報を保持し、この鍵情報保持手段に保持された暗号化鍵情報を、鍵情報送信制御手段の制御により、第２の通信手段によって他の通信装置へ送信するとともに、通信制御手段の制御によって、鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、第１の通信手段によって送信するので、この通信装置により送信される情報は、第２の通信手段によって送信された暗号化鍵情報を受信した通信装置でのみ受信することができる。これにより、第１の通信手段による無線通信について、セキュリティ上の信頼性を確保することができる。特に、第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により情報が受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第２の通信手段によって送信される暗号化鍵情報を受信した通信装置のみに限定できる。従って、通信相手の装置との位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

4

【０００９】請求項２記載の発明は、請求項１記載の通信装置において、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、前記第１の通信手段による無線信号の送受信を拒否する通信拒否手段（例えば、図５のステップＳ４５に示す処理を行うＣＰＵ２１）をさらに備えることを特徴とする。

【００１０】請求項２記載の発明によれば、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、通信拒否手段により、第１の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置を厳格に限定し、情報の秘匿をより確実に保持することができる。

【００１１】請求項３記載の発明は、請求項１または２記載の通信装置において、前記第１の通信手段はブルートゥース（Bluetooth）規格に準じた通信方式により無線信号を送受信するものであって、前記第２の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする。

【００１２】請求項３記載の発明によれば、第１の通信手段はブルートゥース（Bluetooth）規格に準じた通信方式により無線信号を送受信するものであり、第２の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信するので、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第２の通信手段に赤外線信号を用いた通信方式を利用するので、第２の通信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、通信装置は互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

【００１３】請求項４記載の発明は、送信側装置（例えば、図１に示す通信装置２）と受信側装置（例えば、図１に示す通信装置３）とを備えてなる通信システム（１）であって、前記送信側装置は、無線信号を送受信する第１の通信手段（例えば、図１に示す無線通信部２４）と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段（例えば、図１に示す赤外線通信部２６）と、暗号化鍵情報を保持する鍵情報保持手段（例えば、図２に示す原始暗号化情報格納領域１０１を有するメモリ２２）と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第２の通信手段によって前記受信側装置へ送信させる鍵情報送信制御手段（例

5

えば、図３（ａ）に示す処理を行うＣＰＵ２１）と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって前記受信側装置へ送信させる通信制御手段（例えば、図５に示す処理を行うＣＰＵ２１）とを備え、前記受信側装置は、前記送信側装置が有する第２の通信手段により送信された暗号化鍵情報を受信する鍵情報受信手段（例えば、図１に示す赤外線通信部３６、及び図３（ｂ）に示す処理を行うＣＰＵ３１）と、この鍵情報受信手段により受信された暗号化鍵情報を保持する受信鍵情報保持手段（例えば、図１に示すメモリ３２）と、前記送信側装置が有する第１の通信手段により送信された情報を受信する暗号化情報受信手段（例えば、図１に示す無線通信部３４）とを備えることを特徴とする。

【００１４】請求項４記載の発明によれば、送信側装置と受信側装置とを備えてなる通信システムであって、送信側装置は、無線信号を送受信する第１の通信手段と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段とを備え、鍵情報保持手段により暗号化鍵情報を保持し、鍵情報保持手段に保持された暗号化鍵情報を、鍵情報送信制御手段によって、第２の通信手段によって受信側装置へ送信させるとともに、通信制御手段の制御によって、鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、第１の通信手段によって受信側装置へ送信し、受信側装置は、送信側装置が有する第２の通信手段により送信された暗号化鍵情報を鍵情報受信手段によって受信し、鍵情報受信手段により受信された暗号化鍵情報を受信鍵情報保持手段によって保持し、送信側装置が有する第１の通信手段により送信された情報を暗号化情報受信手段によって受信する。

【００１５】また、請求項８記載の発明は、無線信号を送受信する第１の通信手段（例えば、図１に示す無線通信部２４）と、この第１の通信手段とは異なる通信方式により信号を送受信する第２の通信手段（例えば、図１に示す赤外線通信部２６）とを有する送信側装置（例えば、図１に示す通信装置２）と、受信側装置（例えば、図１に示す通信装置３）とを備えてなる通信システム（１）における通信方法であって、前記送信側装置により、暗号化鍵情報を前記第２の通信手段によって前記受信側装置へ送信する工程と、前記受信側装置により、前記送信側装置が有する第２の通信手段により送信された暗号化鍵情報を受信して記憶する工程と、前記送信側装置により、前記暗号化鍵情報をもとに情報を暗号化して、前記第１の通信手段によって前記受信側装置へ送信する工程とを含むことを特徴とする。

【００１６】従って、送信側装置により送信される情報は受信側装置でのみ受信することができる。これにより、送信側装置が有する第１の通信手段を用いた通信システム内の無線通信について、セキュリティ上の信頼性

6

を確保することができる。特に、第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第２の通信手段によって送信される暗号化鍵情報を保持する受信側装置のみに限定できる。従って、互いの装置の位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【００１７】請求項５記載の発明は、請求項４記載の通信システムにおいて、前記送信側装置は、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、前記受信側装置が有する受信鍵情報保持手段に保持されていない場合に、前記第１の通信手段による無線信号の送受信を拒否する通信拒否手段（例えば、図５のステップＳ４５に示す処理を行うＣＰＵ２１）をさらに備えることを特徴とする。

【００１８】請求項５記載の発明によれば、送信側装置は、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、受信側装置が有する受信鍵情報保持手段に保持されていない場合に、通信拒否手段によって、第１の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置をより厳格に限定し、情報の秘匿をより確実に保持することができる。

【００１９】請求項６記載の発明は、請求項４または５記載の通信システムにおいて、前記送信側装置が有する第１の通信手段と、前記受信側装置が有する暗号化情報受信手段とは、ブルートゥース（Bluetooth）規格に準じた通信方式により無線信号を送受信するものであって、前記送信側装置が有する前記第２の通信手段と、前記受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする。

【００２０】請求項６記載の発明によれば、送信側装置が有する第１の通信手段と、受信側装置が有する暗号化情報受信手段とは、ブルートゥース（Bluetooth）規格に準じた通信方式により無線信号を送受信するものであって、送信側装置が有する第２の通信手段と、受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信するので、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第２の通信手段と鍵情報受信手段とは赤外線信号を用いた通信方式を利用するので、第２の通信手段および鍵情報受信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、送信側装置と受信側装置とは互いに

近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

【００２１】請求項７記載の発明は、請求項４から６のいずれかに記載の通信システムにおいて、前記送信側装置が有する鍵情報送信制御手段は、前記暗号化鍵情報を暗号化して前記第２の通信手段によって送信させることを特徴とする。

【００２２】請求項７記載の発明によれば、送信側装置が有する鍵情報送信制御手段は、暗号化鍵情報を暗号化して第２の通信手段によって送信させるので、暗号化鍵情報を送信する際の情報の漏洩をより確実に防止できる。これにより、セキュリティ上の信頼性をより一層高めることができる。

【００２３】

【発明の実施の形態】以下、図を参照して本発明の実施の形態を詳細に説明する。

【００２４】〔第１の実施の形態〕図１は、本発明を適用した第１の実施の形態としての通信システム１の構成を示すブロック図である。同図に示すように、通信システム１は、互いに通信可能な通信装置２及び通信装置３により構成される。通信装置２と通信装置３との間には、無線電波を媒体とする無線通信リンクＡと、赤外線を利用した赤外線通信リンクＢとが形成される。

【００２５】なお、図１に示す通信装置２及び通信装置３は、いずれも同一構成によってなる通信装置であるが、本第１の実施の形態においては、通信装置２をアクセス要求側の装置、通信装置３をアクセス受信側の装置として説明する。

【００２６】通信装置２は、ＣＰＵ（Central Processing Unit）２１、メモリ２２、入力部２３、無線通信部２４、アンテナ２５、赤外線通信部２６、赤外線受発光ユニット２７、及びインターフェース部２８の各部を備えて構成される。

【００２７】ＣＰＵ２１は、入力部２３における指示操作に従って、メモリ２２に格納されたシステムプログラムを読み出して実行し、通信装置２の各部を駆動制御する。具体的には、ＣＰＵ２１は、メモリ２２内のプログラムに従って、無線通信部２４を制御し、通信装置３との間に無線通信リンクＡを確立する。続いてＣＰＵ２１は、赤外線通信部２６及び赤外線受発光ユニット２７によって赤外線通信リンクＢを確立する。そして、ＣＰＵ２１は、赤外線通信リンクＢを介して、メモリ２２内に格納された暗号化に関する各種情報を通信装置３へ送信する。

【００２８】その後、ＣＰＵ２１は、通信装置３から赤外線通信リンクＢを介して送信された情報を受信し、情報の内容を確認して、通信装置３との間の無線通信リンクＡ及び赤外線通信リンクＢを切断する。

【００２９】また、ＣＰＵ２１は、入力部２３から入力される指示に従って、無線通信部２４を制御し、通信装置２の近辺に存在する通信装置をスキャンするための無線信号をアンテナ２５から出力させる。このスキャン動作により、無線通信回線を介して接続可能な通信装置が検出された場合には、検出された通信装置から送信された情報を無線通信部２４によって受信して解析する。

【００３０】そして、受信した情報をメモリ２２内に格納された原始暗号化情報と照合し、一致した場合には接続を許可して、該検出された通信装置との間で無線通信を開始する。また、受信した情報が原始暗号化情報と一致しない場合には、該通信装置との間の通信を拒否する。

【００３１】メモリ２２は、ＥＥＰＲＯＭ、フラッシュメモリ等の不揮発性記憶素子を備えて構成される。メモリ２２は、ＣＰＵ２１により実行されるシステムプログラム等のプログラム、及び、これらプログラムに係るデータ等を格納する。また、メモリ２２は、ＣＰＵ２１により処理されるデータや、入力部２３から入力されたデータ等を一時的に保持する。

【００３２】ここで、メモリ２２に格納されるデータについて説明する。図２は、メモリ２２内部の構成を模式的に示す図である。メモリ２２内には、上記各種プログラムを格納した格納領域（図示略）の他、図２に示すように原始暗号化情報格納領域１０１及び転送諸元情報格納領域１０２が設けられる。

【００３３】原始暗号化情報格納領域１０１には、暗号化の際の「鍵」として使用される暗号化鍵情報、及び、暗号化鍵情報を他の電子機器に対して送信した履歴等を含む暗号化鍵管理情報が格納される。原始暗号化情報格納領域１０１に格納される各種情報を、原始暗号化情報と総称する。

【００３４】この原始暗号化情報格納領域１０１に格納される原始暗号化情報は、予め原始暗号化情報格納領域１０１に格納されているものとしても良いし、入力部２３の操作によって、随時入力されるようにしても良い。

【００３５】また、転送諸元情報格納領域１０２には、通信装置２の製品情報、固有機能情報、使用者情報、シリアルNo.等の各種情報が格納される。これらの転送諸元情報格納領域１０２に格納される各種情報を、転送諸元情報と総称する。なお、転送諸元情報格納領域１０２に格納される情報は、予めメモリ２２に格納されているものとしても良いし、入力部２３の操作によって入力されるものとしても良く、或いは、インターフェース部２８に接続された電子機器４から入力されるものとしても良い。

【００３６】入力部２３は、それぞれ入力可能な情報が割り当てられた複数のキー等の入力デバイスを備えており、操作内容に対応する操作信号を生成してＣＰＵ２１へ出力する。

【００３７】無線通信部２４は、エンコーダ、デコーダ、ＲＦ、アンプ等を内蔵しており、ＣＰＵ２１から入

9

力される信号を変換して無線信号を生成し、アンテナ２５を介して通信装置３へ送信する。また、無線通信部２４は、通信装置３から送信された無線信号をアンテナ２５によって受信し、受信した無線信号を変換して得られる信号をＣＰＵ２１へ出力する。

【００３８】ここで、無線通信部２４としては、例えば、ブルートゥース（Bluetooth）規格に準じた無線通信ユニットが挙げられる。Bluetooth規格とは、通信機器、電子機器、ソフトウェア等を製造する事業者が複数集まって構成されるプロモーターと、Bluetooth SIG（Special InterestGroup）により策定された無線通信規格である。Bluetooth規格では、2.4GHz（ギガヘルツ）帯の周波数の無線信号を利用して、およそ数メートル以内の複数の電子機器間で無線通信を行う。

【００３９】Bluetooth規格に準じた無線通信ユニットを搭載した電子機器は、互いにピコネットと呼ばれるグループを形成する。そして、同一のピコネットに属する電子機器間で相互に通信することが可能である。同一のピコネットには多くの電子機器が同時に属することができる。また、１台の通信装置が同時に複数のピコネットに属することも可能である。このため、携帯型電話機を始め、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant）と呼ばれるハンドヘルドコンピュータ、プリンタ、音楽プレーヤ等の様々な機器を互いに接続する通信方式として注目されている。以下、無線通信部２４は上記Bluetooth規格に準じた通信ユニットであり、無線通信部２４及びアンテナ２５を利用して実行される無線通信（無線通信リンクＡを介した無線通信）は、Bluetooth規格に準じた2.4GHz帯の電波により行われるものとして説明する。

【００４０】赤外線通信部２６は、エンコーダ、デコーダ等を内蔵しており、赤外線受発光ユニット２７に接続されている。赤外線通信部２６は、ＣＰＵ２１から入力された信号を変換して赤外線受発光ユニット２７へ出力する。赤外線受発光ユニット２７は、ＬＥＤ（Light Emitting Diode）やフォトセンサ等を内蔵し、赤外線通信部２６から入力された信号をもとに内蔵するＬＥＤを発光させ、赤外線信号として通信装置３へ向けて出力する。

【００４１】また、赤外線受発光ユニット２７は、内蔵するフォトセンサによって通信装置３からの赤外光を受光すると、受光パターンを所定の信号に変換して赤外線通信部２６へ出力する。さらに、赤外線通信部２６は、赤外線受発光ユニット２７から入力される信号を変換して、ＣＰＵ２１へ出力する。

【００４２】インターフェース部２８は、通信装置２と、通信装置２の外部の電子機器とを接続するためのインターフェースであって、コネクタ等を備えている。ここで、インターフェース部２８に接続される電子機器５としては、例えば、携帯型電話機やパーソナルコンピュータ、ＰＤＡ等が挙げられるが、特に限定されるものではない。また、通信装置２は、図示しないリチウムイオン電池やニッケルーカドミウム電池等の二次電池、もしくは乾電池等を内蔵し、これらの電池を電源として動作するが、通信装置２に電池を内蔵せずに、インターフェース部２８を介して通信装置２へ電源が供給される構成としても良い。

10

【００４３】さらに、通信装置２が有する入力部２３に代えて、インターフェース部２８に接続された機器が具備する入力装置を用いる構成としても良い。この場合、ＣＰＵ２１は、インターフェース部２８に接続された機器から入力される信号に従って動作すれば良く、入力部２３を備えていなくても良い。

【００４４】次いで、通信装置３の構成について説明する。通信装置３は、ＣＰＵ３１、メモリ３２、入力部３３、無線通信部３４、アンテナ３５、赤外線通信部３６、赤外線受発光ユニット３７、及びインターフェース部３８の各部を備えて構成される。ここで、上記メモリ３２、入力部３３、無線通信部３４、アンテナ３５、赤外線通信部３６、赤外線受発光ユニット３７、及びインターフェース部３８の各部は、通信装置２が有するメモリ２２、入力部２３、無線通信部２４、アンテナ２５、赤外線通信部２６、赤外線受発光ユニット２７、及びインターフェース部２８の各部と同一の構成によってなるものであり、説明を省略する。

【００４５】ＣＰＵ３１は、入力部３３における指示操作に従って、メモリ３２に格納されたシステムプログラムを読み出して実行し、通信装置３の各部を駆動制御する。具体的には、ＣＰＵ３１は、メモリ３２内のプログラムに従って、無線通信部３４を制御し、通信装置２との間に無線通信リンクＡを確立する。

【００４６】続いてＣＰＵ３１は、赤外線通信部３６及び赤外線受発光ユニット３７によって赤外線通信リンクＢを確立する。そして、ＣＰＵ３１は、通信装置２が有する赤外線受発光ユニット２７から発せられた赤外線信号を赤外線受発光ユニット３７によって受光し、通信装置２から送信された暗号化に関する各種情報を受信する。

【００４７】ここで、ＣＰＵ３１は、通信装置２から送信された各種情報をメモリ３２内に格納するとともに、該情報を、赤外線通信部３６及び赤外線受発光ユニット３７を介して通信装置２へ送信する。そして、通信装置２が有するアンテナ２５から出力された無線信号を受信し、受信した信号が無線通信リンクＡ及び赤外線通信リンクＢの切断を要求している場合は、通信装置２との間の無線通信リンクＡ及び赤外線通信リンクＢを切断する。

【００４８】次に、本実施の形態の動作を説明する。図３は、本第１の実施の形態における通信システム１の動作を示すフローチャートである。図３（ａ）は、アクセ

ス要求側の装置、すなわち通信装置２の動作を示し、図３（ｂ）はアクセス受信側の装置、すなわち通信装置３の動作を示す。なお、図中、実線矢印で示す信号は、無線通信リンクＡ（図１）を介して送受信される上記Bluetooth規格に準じた無線信号であり、破線矢印で示す信号は、赤外線通信リンクＢ（図１）を介して送受信される赤外線信号である。

【００４９】まず、図３（ａ）に示すように、ＣＰＵ２１は、入力部２３からの指示入力に従って動作を開始し、通信装置３に対して接続を求める接続要求信号を生成して、無線通信部２４によって通信装置３へ送信させる（ステップＳ１１）。

【００５０】ＣＰＵ３１は、入力部３３からの指示入力によって動作を開始し、無線通信部３４によって通信装置２から送信される無線信号を受信可能な状態に移行する。そして、無線通信部２４から送信された接続要求を無線通信部３４によって受信すると（ステップＳ２１）、接続の確認となる接続確認信号を生成し、無線通信部３４によって送信させる（ステップＳ２２）。

【００５１】ＣＰＵ２１は、ＣＰＵ３１の制御により無線通信部３４から送信された接続確認信号を無線通信部２４によって受信すると（ステップＳ１２）、メモリ２２の転送諸元情報格納領域１０２に格納された転送諸元情報を読み出して、赤外線通信部２６及び赤外線受発光ユニット２７によって、赤外線信号として通信装置３へ送信させる（ステップＳ１３）。

【００５２】ＣＰＵ３１は、通信装置２の赤外線通信部２６により赤外線信号として送信された転送諸元情報を、赤外線通信部３６によって受信すると（ステップＳ２３）、メモリ３２の転送諸元情報格納領域１０２に格納された転送諸元情報を読み出して、赤外線通信部３６によって送信させる（ステップＳ２４）。

【００５３】ＣＰＵ２１は、通信装置３から送信された転送諸元情報を赤外線通信部２６によって受信すると（ステップＳ１４）、メモリ２２内の原始暗号化情報格納領域１０１に格納されている原始暗号化情報を読み出して、赤外線通信部２６によって通信装置３へ送信させる（ステップＳ１５）。

【００５４】ＣＰＵ３１は、通信装置２から送信された原始暗号化情報を受信すると（ステップＳ２５）、受信した原始暗号化情報をメモリ３２内の原始暗号化情報格納領域１０１に記憶させる（ステップＳ２６）。なお、ここで、予めメモリ３２の原始暗号化情報格納領域１０１に格納されていた原始暗号化情報については、新たに受信した原始暗号化情報により上書きされるものとしても良いし、或いは、新たに受信した原始暗号化情報とは異なる領域に保存されるものとしても良い。

【００５５】続いて、ＣＰＵ３１は、ステップＳ２５で受信し、メモリ３２内の原始暗号化情報格納領域１０１に記憶した原始暗号化情報を、赤外線通信部３６によって通信装置２へ送信する（ステップＳ２７）。

【００５６】ＣＰＵ２１は、通信装置３から送信された原始暗号化情報を受信すると（ステップＳ１６）、受信した原始暗号化情報と、メモリ２２の原始暗号化情報格納領域１０１に格納されている原始暗号化情報とを照合し、一致することを確認する（ステップＳ１７）。すなわち、ステップＳ１５で通信装置３へ送信した原始暗号化情報と、通信装置３から送信された原始暗号化情報とが一致することを確認することにより、ステップＳ１５，Ｓ１６，Ｓ２５，Ｓ２６における原始暗号化情報の送受信が問題なく実行されたことを確認する。

【００５７】そして、ＣＰＵ２１は、通信の切断を要求する切断要求信号を生成して、無線通信部２４によって通信装置３へ送信させる（ステップＳ１８）。ＣＰＵ３１は、通信装置２から送信された切断要求信号を無線通信部３４によって受信すると（ステップＳ２８）、切断要求の受信を確認する切断確認信号を生成して、無線通信部３４によって通信装置２へ送信させ（ステップＳ２９）、本処理を終了する。

【００５８】また、ＣＰＵ２１は、通信装置３から送信された切断確認信号を無線通信部２４によって受信すると（ステップＳ１９）、本処理を終了する。

【００５９】以上の図３に示す処理によって、通信装置２が有するメモリ２２と、通信装置３が有するメモリ３２とは、予めメモリ２２内の原始暗号化情報格納領域１０１に格納されていた原始暗号化情報を格納した状態になる。

【００６０】図３に示す処理においては、転送諸元情報および原始暗号化情報が、赤外線通信リンクＢ（図１）を介して送受信される。一般に、赤外線信号による無線通信を行う場合、通信を行う電子機器が互いに近接しており、かつ、互いの電子機器が有する赤外線受発光部が対向していることが必要である。特に、互いの電子機器が有する赤外線受発光部は、比較的狭い立体角に収まるように対向していなければならず、無関係な電子機器により傍受される可能性は低く、セキュリティ上の懸念は小さいものである。しかしながら、以下に述べる暗号化を施すことにより、赤外線通信リンクＢを介した通信におけるセキュリティ上の信頼性をより確実なものとすることができる。

【００６１】図４（ａ）には、暗号化を施す際の赤外線通信におけるプロトコル構成を示す階層モデルを図示する。また、図４（ｂ）には、赤外線通信におけるデータユニットの構成を模式的に示す。

【００６２】一般に、赤外線通信においては、データリンク層、リンクマネージメント層、トランスポート層における互換性を保持していれば、それより上位の階層におけるサービス・データ・ユニットを暗号化しても、プロトコル互換性を保つことができる。従って、図４（ａ）に示すように、トランスポート層よりも上位の層

を暗号化層とし、さらにその上位層を、前述の転送諸元情報や原始暗号化情報を交換するセキュリティデータ交換プロトコル層とすれば、プロトコル互換性を保ちながら、転送される情報の秘匿性を保つことができる。

【００６３】具体的には、図４（ｂ）に示すように、ＬＡＰ（データリンク層）、ＬＭＰ（リンクマネージメント層）、及びＴＰ（トランスポート層）のプロトコルデータユニットに続くサービス・データ・ユニットを暗号化すれば良い。従って、通信装置２及び通信装置３の双方において、赤外線通信リンクＢを介して送受信する信号の暗号化及び復号を行うことにより、図３に示す処理で送受信される転送諸元情報や原始暗号化情報の秘匿性をより確実なものとすることができる。

【００６４】図５は、図３に示す処理の実行後における通信装置２の動作を示すフローチャートである。この図５に示す処理において、通信装置２は、Bluetooth規格により規定されるMasterのデバイスとして動作する。また、図５に示す処理において送受信される無線信号は、Bluetooth規格に準じた2.4GHz帯の無線信号である。

【００６５】まず、ＣＰＵ２１は、入力部２３から入力される指示に従って動作を開始し、無線通信部２４を制御してPage Scan動作を実行し、Bluetooth規格に準じた通信が可能な通信装置を検出する（ステップＳ４１）。

【００６６】そして、接続可能な通信装置を検出した場合は、ＣＰＵ２１によるPage Scan動作に応じて検出した装置から送信された情報を受信し（ステップＳ４２）、受信した情報と、メモリ２２内の原始暗号化情報格納領域１０１に格納されている原始暗号化情報との照合を行う（ステップＳ４３）。

【００６７】ここで、通信装置２が通信装置３を検出した場合、通信装置３は、メモリ２２内の原始暗号化情報格納領域１０１に格納されている原始暗号化情報を既に保持しているため、Page Scan動作に応じて原始暗号化情報に従って暗号化された情報を送信する。また、通信装置２及び通信装置３とは無関係な通信装置が検出された場合は、この無関係な通信装置からは、Page Scan動作に応じて通常の無線信号が送信される。従って、ステップＳ４３における照合により、ステップＳ４１で検出した通信装置が通信装置３であるか否かを判別できる。

【００６８】ステップＳ４３における照合の結果、ステップＳ４２で受信した無線信号が原始暗号化情報とは無関係であった場合は（ステップＳ４４；Ｎｏ）、ＣＰＵ２１は、検出した通信装置との接続を拒否し（ステップＳ４５）、本処理を終了する。

【００６９】また、ステップＳ４３での照合により、ステップＳ４２で受信した無線信号が原始暗号化情報に適合した場合は（ステップＳ４４；Ｙｅｓ）、ＣＰＵ２１は、検出した通信装置との間で、原始暗号化情報格納領域１０１内の原始暗号化情報により暗号化された無線信号の送受信を開始する（ステップＳ４６）。なお、原始暗号化情報格納領域１０１に格納された原始暗号化情報により暗号化された情報は、該原始暗号化情報をもとに復号できる。このため、ＣＰＵ２１は、無線通信部２４により送信する情報を暗号化するとともに、無線通信部２４により受信した情報を復号する。

【００７０】そして、ＣＰＵ２１は、検出した通信装置との間のネゴシエーションが終了してからアプリケーションでの使用を許可する（ステップＳ４７）。その後、ＣＰＵ２１は、通信装置２、もしくはインターフェース部２８に接続された電子機器４上で実行されるアプリケーションプログラムの要求に応じて、暗号化された無線信号を送受信する処理を実行し（ステップＳ４８）、入力部２３からの指示入力によって本処理を終了する。

【００７１】以上のように、本発明の第１の実施の形態によれば、Bluetooth規格に準じた無線通信を行う無線通信部２４及びアンテナ２５と、赤外線信号を用いた無線通信を行う赤外線通信部２６及び赤外線受発光ユニット２７とを備える通信装置２と、通信装置２と同一構成によってなる通信装置３との間において、予め赤外線通信によって原始暗号化情報を転送し、その後、転送した原始暗号化情報に基づいて暗号化された情報を、Bluetooth規格に準じた無線通信で送受信する。これにより、高い秘匿性を保ちながら、Bluetooth規格に準じた利便性の高い通信を行うことができる。

【００７２】すなわち、Bluetooth規格に準じた無線通信を利用した場合、互いの通信装置を近接させるだけでピコネットを形成して通信を開始できる。また、通信中の各通信機器は、同時に他の通信装置との間においてピコネットを形成することができ、フレキシブルな通信を行うことができる。さらに、ピコネットを形成する通信装置は、互いに所定の距離以内に近接していれば良く、位置が拘束されることが少ない。その反面、Bluetooth規格に準じた無線通信では、特定の通信装置に対してのみ情報を送信することが難しく、誤って無関係な通信装置に受信されてしまう可能性が否定できない。しかしながら、上記第１の実施の形態における通信システム１によれば、予め通信装置２と通信装置３との間で、赤外線通信によって原始暗号化情報を転送することにより、無関係な通信装置に影響されることなく原始暗号化情報を共有し、この原始暗号化情報を用いて暗号化された情報を、Bluetooth規格に準じた無線通信で送受信する。従って、セキュリティ上の信頼性を確保しながら、利便性の高い無線通信を行うことができる。

【００７３】なお、上記実施の形態においては、通信装置２と通信装置３とは、Bluetooth規格に準じた無線通信リンクＡを介して無線通信を行うものとしたが、本発明はこれに限定されるものではなく、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に対しても適用可能であり、上記の通信システム１と同様の効果を奏するものである。

15

【００７４】さらに、携帯型電話機やＰＤＡ、パーソナルコンピュータ、プリンタ、音楽プレーヤ等の各種電子機器に本発明を適用する場合は、図１に示したような通信装置２及び通信装置３に対して電子機器４，５が接続される構成に限らず、上記各種電子機器に、通信装置２，３の機能を内蔵させることも勿論可能である。

【００７５】また、上記第１の実施の形態においては、通信装置２及び通信装置３はいずれも入力部２３，３３を具備しており、これら入力部２３，３３における指示入力によって図３に示す処理を開始するものとしたが、必ずしも入力部２３，３３を備える構成でなくても良い。以下、この場合について第２の実施の形態として説明する。

【００７６】〔第２の実施の形態〕図６は、本発明の第２の実施の形態における通信システム１０の構成を示すブロック図である。

【００７７】同図に示すように、通信システム１０は、通信装置２と、通信装置３ａとによって構成される。通信システム１０は、通信装置３ａが有するメモリ６１およびスイッチ６２を除いては、上記第１の実施の形態における通信システム１と同様の構成によってなるものであり、共通部分については同符号を付して説明を省略する。

【００７８】スイッチ６２は、１個もしくは複数のスイッチを備えており、操作される毎に操作信号を生成してＣＰＵ３１へ出力する。

【００７９】図７は、メモリ６１の内部構成を模式的に示す図である。同図に示すように、メモリ６１内には、原始暗号化情報格納領域１０３及び転送諸元情報格納領域１０２が設けられており、転送諸元情報格納領域１０２には製品情報、固有機能情報、使用者情報、シリアルNo.等の転送諸元情報が格納されている。一方、原始暗号化情報格納領域１０３には、事前に原始暗号化情報は格納されていない。

【００８０】上記第１の実施の形態で説明した通信システム１では、図３に示す処理において、通信装置２から通信装置３へ原始暗号化情報が転送され、メモリ２２の原始暗号化情報格納領域１０１に格納されていた原始暗号化情報が、メモリ３２の原始暗号化情報格納領域１０１に格納される。本第２の実施の形態における通信システム１０では、通信装置２から通信装置３ａへ原始暗号化情報が転送されると、転送された原始暗号化情報はメモリ６１の原始暗号化情報格納領域１０３へ格納される。従って、通信装置３ａは、上記通信装置３と同様に動作することができる。

【００８１】また、上記第１の実施の形態で説明した通信システム１では、通信装置２が有する入力部２３および通信装置３が有する入力部３３における指示入力により、図３に示す処理が開始されるものとした。本第２の実施の形態における通信システム１０では、通信装置２が有する入力部２３における指示入力、及び、通信装置３ａが有するスイッチ６２のスイッチ操作によって、図３に示す処理と同様の処理が実行される。

16

【００８２】すなわち、通信装置３ａは、入力手段としてスイッチ６２のみを備える装置であるが、上記第１の実施の形態における通信装置３に代えて、通信装置２によるアクセスを受信する動作のみを行う装置として使用可能である。また、通信装置２に代えてアクセス要求側の装置として利用しないため、メモリ６１の原始暗号化情報格納領域１０３には予め原始暗号化情報を格納する必要がない。

【００８３】従って、本第２の実施の形態における通信システム１０は、入力スイッチ６２のみを有する通信装置３ａを用いて、上記第１の実施の形態と同様の効果を奏するものである。これにより、Bluetooth規格に準じた無線通信において、Slaveのデバイスとしてのみ機能する装置には、入力手段としては単なるスイッチを備えるだけで、通信システム１と同様の効果を得ることができる。

【００８４】

【発明の効果】請求項１記載の発明の通信装置によれば、送信される情報は、第２の通信手段によって送信された暗号化鍵情報を受信した通信装置でのみ受信可能となる。これにより、第１の通信手段による無線通信について、セキュリティ上の信頼性を確保することができる。特に、第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第２の通信手段によって送信される暗号化鍵情報を受信した通信装置のみに限定できる。従って、通信相手の装置との位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【００８５】請求項２記載の発明の通信装置によれば、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、通信拒否手段により、第１の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置を厳格に限定し、情報の秘匿をより確実に保持することができる。

【００８６】請求項３記載の発明の通信装置によれば、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第２の通信手段に赤外線信号を用いた通信方式を利用するので、第２の通信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能であ

17

る。また、赤外線信号を用いた通信方式では、通信装置は互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

【００８７】請求項４記載の発明の通信システム、及び、請求項８記載の発明の通信方法によれば、送信側装置により送信される情報は受信側装置でのみ受信することができる。これにより、送信側装置が有する第１の通信手段を用いた通信システム内の無線通信について、セキュリティ上の信頼性を確保することができる。特に、第１の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第２の通信手段によって送信される暗号化鍵情報を保持する受信側装置のみに限定できる。従って、互いの装置の位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【００８８】請求項５記載の発明の通信システムによれば、送信側装置は、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、受信側装置が有する受信鍵情報保持手段に保持されていない場合に、通信拒否手段によって、第１の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置をより厳格に限定し、情報の秘匿をより確実に保持することができる。

【００８９】請求項６記載の発明の通信システムによれば、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース（Bluetooth）規格の無線通信において、情報の秘匿性を確保することができる。特に、第２の通信手段と鍵情報受信手段とは赤外線信号を用いた通信方式を利用するので、第２の通信手段および鍵情報受信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、送信側装置と受信側装置とは互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

18

【００９０】請求項７記載の発明の通信システムによれば、送信側装置が有する鍵情報送信制御手段は、暗号化鍵情報を暗号化して第２の通信手段によって送信させるので、暗号化鍵情報を送信する際の情報の漏洩をより確実に防止できる。これにより、セキュリティ上の信頼性をより一層高めることができる。

【図面の簡単な説明】

【図１】本発明を適用した第１の実施の形態における通信システム１の構成を示すブロック図である。

【図２】図１のメモリ２２，３２の内部構成を模式的に示す図である。

【図３】図１の通信システム１の動作を示すフローチャートであり、（ａ）は通信装置２の動作を示し、（ｂ）は通信装置３の動作を示す。

【図４】図３に示す処理に暗号化を施した場合のプロトコル構成を示す説明図であり、（ａ）は暗号化を施す際の赤外線通信におけるプロトコル構成を示す階層モデルを示し、（ｂ）は、赤外線通信におけるデータユニットの構成を模式的に示す。

【図５】図１の通信装置２によりBluetooth規格に準じた無線通信を行う際の動作を示すフローチャートである。

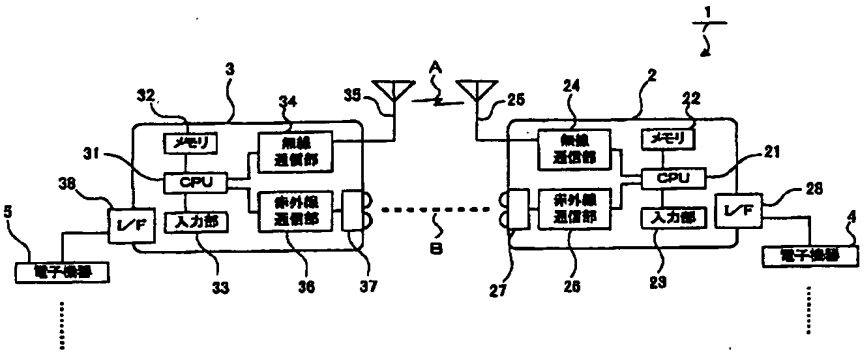
【図６】本発明を適用した第２の実施の形態における通信システム１０の構成を示すブロック図である。

【図７】図６に示すメモリ６１の内部構成を模式的に示す図である。

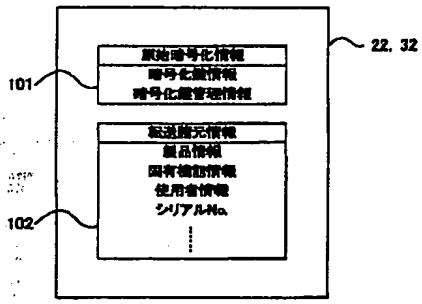
【符号の説明】

１，１０　通信システム
２，３　通信装置
２１，３１　ＣＰＵ
２２，３２　メモリ
２３，３３　入力部
２４，３４　無線通信部
２５，３５　アンテナ
２６，３６　赤外線通信部
２７，３７　赤外線受発光ユニット
２８，３８　インターフェース部
６１　メモリ
６２　スイッチ
１０１，１０３　原始暗号化情報格納領域
１０２　転送諸元情報格納領域

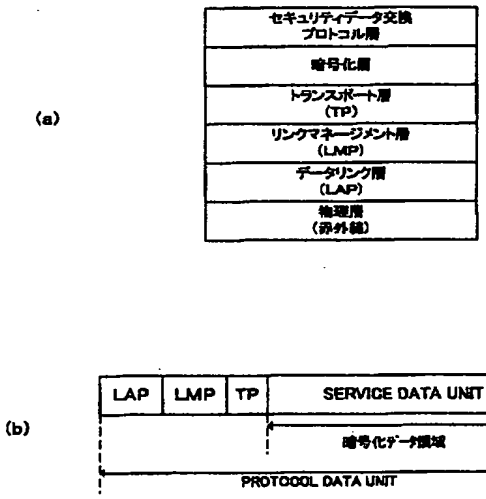
【図１】


1
3
32
34
35
A
25
24
2
22
31
メモリ
無線通信部
メモリ
CPU
CPU
21
38
28
5
レイヤF
入力部
赤外線通信部
赤外線通信部
入力部
レイヤF
4
電子機器
B
電子機器
33
36
37
27
26
23

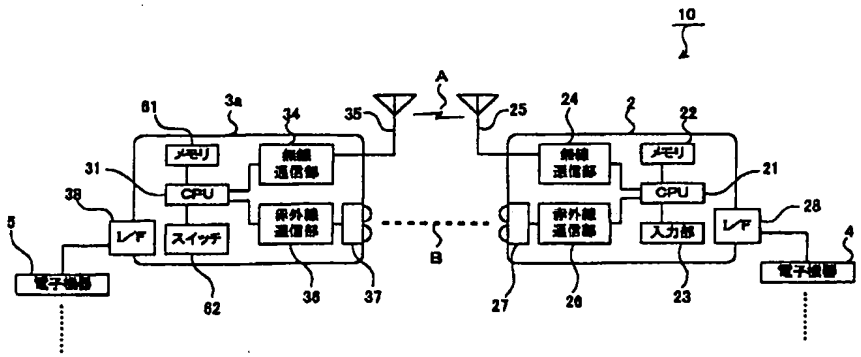
【図２】


22, 32
101
暗号化鍵情報
暗号化鍵管理情報
102
製品情報
固有識別情報
使用者情報
シリアルNo.

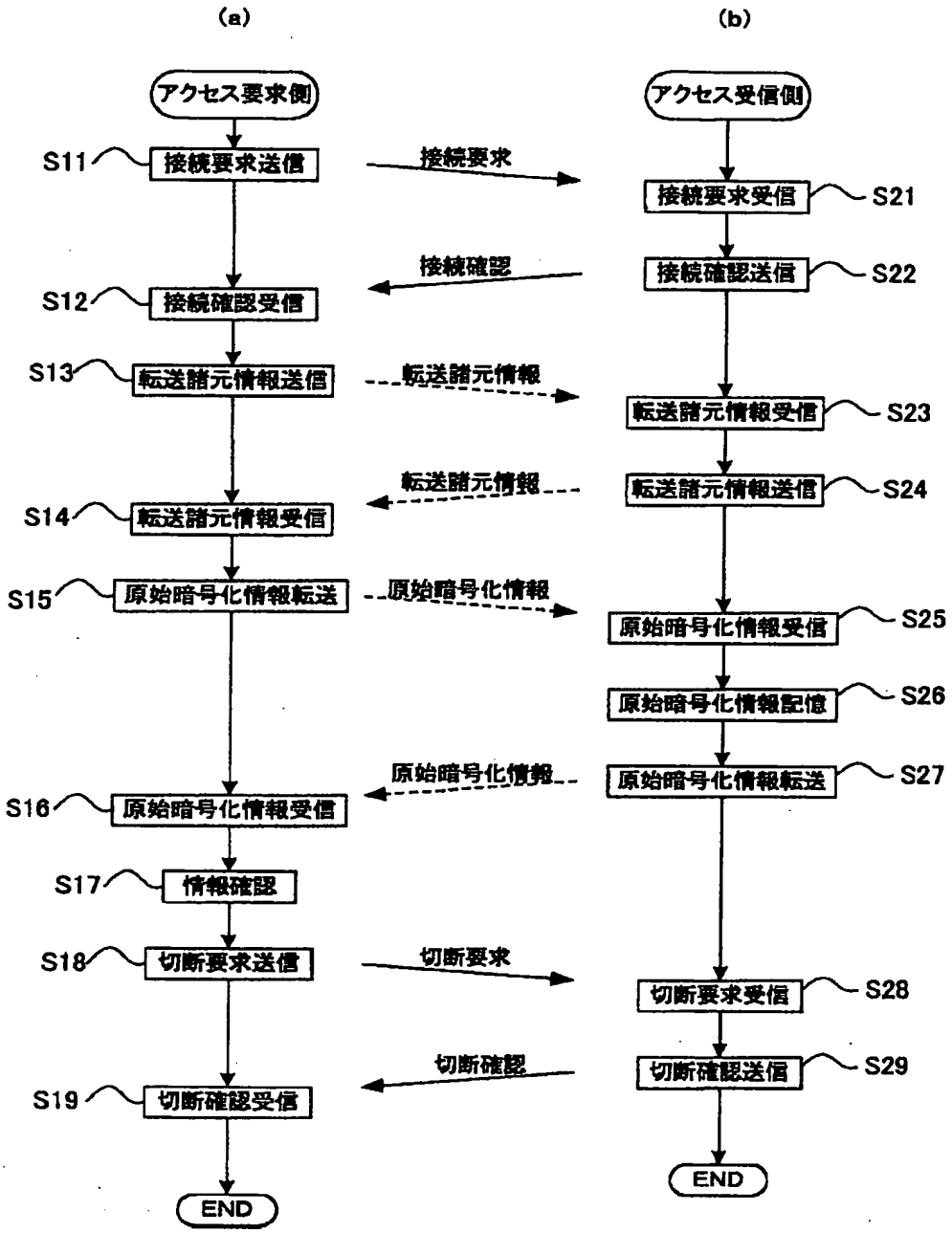
【図４】


(a)
セキュリティデータ交換プロトコル層
暗号化層
トランスポート層 (TP)
リンクマネージメント層 (LMP)
データリンク層 (LAP)
物理層 (赤外線)
(b)
LAP
LMP
TP
SERVICE DATA UNIT
暗号化データ領域
PROTOCOL DATA UNIT

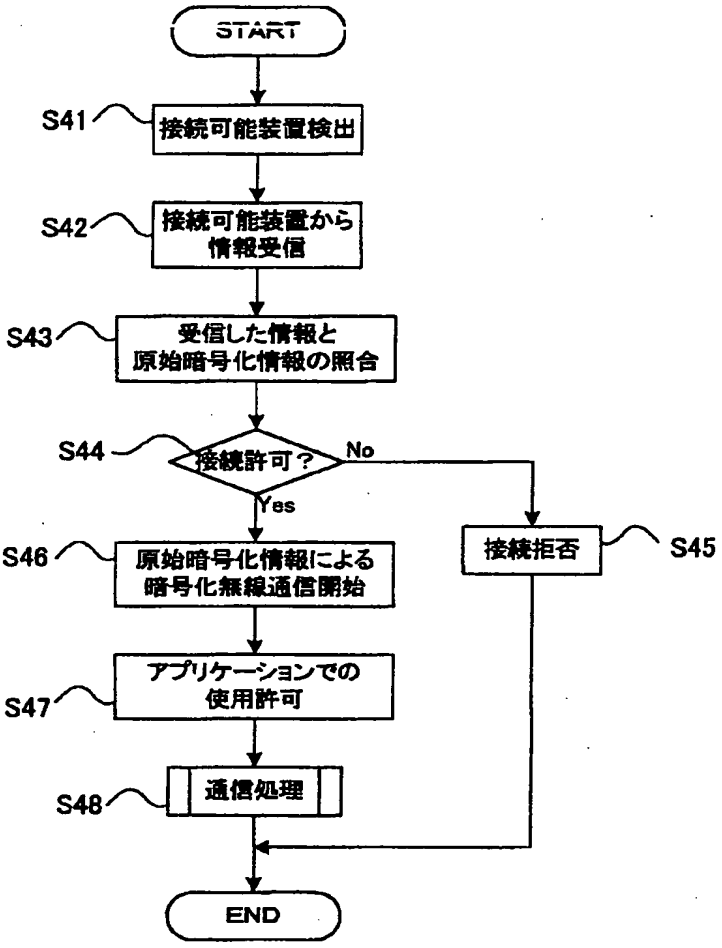
【図６】


10
A
61
3a
34
35
25
24
2
22
31
メモリ
無線通信部
メモリ
CPU
CPU
21
38
28
5
レイヤF
スイッチ
赤外線通信部
赤外線通信部
入力部
レイヤF
4
電子機器
B
電子機器
62
36
37
27
26
23

【図３】


(a)
(b)
アクセス要求側
アクセス受信側
S11
接続要求送信
接続要求
接続要求受信
S21
接続確認
接続確認送信
S22
S12
接続確認受信
S13
転送諸元情報送信
転送諸元情報
転送諸元情報受信
S23
転送諸元情報
転送諸元情報送信
S24
S14
転送諸元情報受信
S15
原始暗号化情報転送
原始暗号化情報
原始暗号化情報受信
S25
原始暗号化情報記憶
S26
原始暗号化情報
原始暗号化情報転送
S27
S16
原始暗号化情報受信
S17
情報確認
S18
切断要求送信
切断要求
切断要求受信
S28
切断確認
切断確認送信
S29
S19
切断確認受信
END
END

【図５】


START
S41
接続可能装置検出
S42
接続可能装置から情報受信
S43
受信した情報と原始暗号化情報の照合
S44
接続許可？
No
Yes
S45
接続拒否
S46
原始暗号化情報による暗号化無線通信開始
S47
アプリケーションでの使用許可
S48
通信処理
END

【図７】